MARCO DE POLÍTICAS DEL SGSI

1. Política SGSI

INTEGRA WEB, como organización proveedora de servicios de desarrollo de software y de Software como servicio, tiene un compromiso decidido hacia la calidad de su producto y la seguridad de la información propia y de terceros que se la hayan confiado, incluyendo los de carácter personal, deber que incluye al personal que actúa en nombre de la empresa, así como toda parte interesada que pueda tener acceso a dicha información.

El Sistema de gestión de la Información en la organización está basado en la gestión de riesgos y su arquitectura de control la cual incluye medidas preventivas y reactivas de la organización y de los sistemas tecnológicos para proteger así la información en aras de lograr los objetivos de negocio mientras mantiene su confidencialidad, disponibilidad e integridad. La organización realizará evaluaciones periódicas de riesgos y actualizará los controles implementados conforme a los resultados obtenidos y a los cambios en el entorno tecnológico, normativo y de negocio.

Nuestro compromiso reúne la gestión del cumplimiento y de la conformidad sobre los requisitos aplicables, tanto del ordenamiento jurídico pertinente, como contractual y técnico, haciendo especial énfasis en los aspectos de privacidad, transparencia y nivel de servicio, así como de la protección adecuada de información de carácter reservado.

En el marco de nuestra implementación de la norma ISO 27001, asumimos un compromiso firme con la eficacia y la mejora continua de nuestro Sistema de Gestión de Seguridad de la Información (SGSI). Este compromiso implica una dedicación constante a la protección de la información, la identificación de riesgos y oportunidades, y la adaptación proactiva de nuestros procesos y controles de seguridad. Para lograr la eficacia, establecemos políticas y procedimientos claros para gestionar la seguridad de la información en toda la organización. Además, asignamos roles y responsabilidades definidas para garantizar que todos los miembros del equipo estén alineados con nuestros objetivos de seguridad.

La mejora continua es un principio esencial en nuestro enfoque de gestión de seguridad. Regularmente evaluamos nuestro SGSI a través de auditorías internas y revisiones de dirección. Estas evaluaciones nos permiten identificar áreas de mejora y oportunidades para fortalecer nuestro sistema. Además, fomentamos una cultura de seguridad de la información en la organización, promoviendo la formación y la concienciación entre los empleados. La retroalimentación de los empleados y las partes interesadas es vital para impulsar mejoras continuas en nuestro SGSI.

Nuestro compromiso con la eficacia y la mejora continua según ISO 27001 nos guía en la protección de la información y en la adaptación constante de nuestro sistema para enfrentar los desafíos cambiantes de seguridad. Esto nos permite mantener la confianza de nuestros clientes, socios y partes interesadas en la seguridad de su información.

2. Politica de Calidad

INTEGRA WEB establece su Política de Calidad como marco de referencia para garantizar la prestación de servicios tecnológicos que satisfagan los requisitos de los clientes y de las partes interesadas, cumpliendo los requisitos legales, contractuales y normativos aplicables.

La organización orienta sus actividades hacia la mejora continua del Sistema de Gestión de Calidad, el fortalecimiento de la eficiencia de sus procesos y el desarrollo de soluciones tecnológicas confiables, seguras y de alto valor para sus clientes.

Esta política proporciona el marco de referencia para el establecimiento, seguimiento y revisión de los objetivos de calidad, los cuales serán definidos por la alta dirección y estarán alineados con la estrategia organizacional, el contexto de la organización y las necesidades de las partes interesadas.

3. Política para los dispositivos móviles

INTEGRA WEB, para la gestión integral en relación con su alcance respecto de los dispositivos móviles, ha establecido las siguientes directrices considerando los requisitos aplicables conforme a lo declarado en la política general integral y bajo un enfoque aplicado de mejora continua y de gestión integral del riesgo:

ELEMENTO DEL ALCANCE	Procesamiento	Consulta	Almacenaje	
a. Prestación servicios de gestión de la información y sistemas de información (Software como servicios)	Permitido/in situ + offsite		Permitido con inspección	Portátiles
	Permitido/in situ + offsite		Permitido con inspección	iPad/Tablet
	Permitido/in situ		No permitido	Smartphone
	No permitido		No permitido	HDD externo
b. Administración delegada de infraestructura tecnológica, de hardware y de software, propia y/o de terceros	Permitido/in situ + offsite		Permitido con inspección	Portátiles
	No permitido		No permitido	iPad/Tablet
	No permitido		No permitido	Smartphone
	No permitido		No permitido	HDD externo
c. Ingeniería de software	Permitido/in situ + offsite		No permitido	Portátiles
	Permitido/in situ + offsite		No permitido	iPad/Tablet
	Permitido/in situ + offsite		No permitido	Smartphone
	No permitido		No permitido	HDD externo

1. Los dispositivos móviles autorizados para contener información de la compañía deben estar registrados en el inventario de activos de información.
2. Los celulares deben contar con clave y bloqueo automático.
3. Existe un listado de dispositivos móviles corporativos autorizados para ser retirados de la compañía.
4. No modificar las configuraciones de seguridad, software o hardware de los dispositivos móviles corporativos bajo su responsabilidad.
5. Evitar la instalación de programas desde fuentes desconocidas; se deben instalar aplicaciones únicamente desde los repositorios oficiales de los dispositivos móviles.
6. No hacer uso de redes inalámbricas de uso público, así como deben desactivar las redes inalámbricas como Wifi, Bluetooth, en los dispositivos móviles.

7. No conectar los dispositivos móviles por puerto USB a cualquier computador público, de hoteles, internet, entre otros.
8. No almacenar videos, fotografías o información personal en los dispositivos móviles corporativos.

4. Política de uso de controles criptográficos y gestión de llaves.

- INTEGRA WEB, con el fin de garantizar la disponibilidad, integridad y confidencialidad de la gestión segura de la información ha determinado realizar cifrado en los discos duros y utilizar plantilla de WordPress con certificado SSL para el sitio web.
- INTEGRA WEB, adaptándose al contexto actual de la pandemia del Covid 19 ha permitido trabajar desde computadores personales y por tanto, no se continúa con el cifrado de discos duros.
- INTEGRA WEB, luego de cumplir todos los protocolos y procedimientos para la pandemia del Covid 19 se mantiene bajo la modalidad de trabajo hibrido remoto y presencial para los trabajadores de la empresa.
- INTEGRA WEB, con el fin de asegurar las contraseñas de Wifi, serán cambiadas cada tres meses.
- Se realizarán revisiones de forma periódica (anualmente) en los controles criptográficos.
- INTEGRA WEB implementa controles criptográficos orientados a proteger la confidencialidad, integridad y disponibilidad de la información tratada por la organización.
- Las comunicaciones electrónicas que involucren información sensible o datos personales se realizan mediante protocolos seguros (TLS 1.2 o superior).
- La información almacenada en plataformas de servicio (SaaS, bases de datos y repositorios corporativos) cuenta con mecanismos de protección conforme a las capacidades técnicas del proveedor de infraestructura.
- En los equipos utilizados para el tratamiento de información, se aplican medidas de seguridad como autenticación segura, control de acceso basado en roles y bloqueo automático por inactividad.
- INTEGRA WEB evaluará periódicamente la necesidad de fortalecer los mecanismos criptográficos implementados, conforme a la evolución tecnológica, análisis de riesgos y requisitos normativos.
- Las contraseñas de redes inalámbricas corporativas serán cambiadas periódicamente y gestionadas bajo criterios de seguridad definidos por la organización.
- INTEGRA WEB realizará revisiones anuales de los controles criptográficos implementados, como parte del proceso de mejora continua del SGSI.

5. Política de teletrabajo

INTEGRA WEB, para la gestión integral en relación con su alcance respecto del teletrabajo, ha establecido lo siguiente considerando los requisitos aplicables conforme a lo declarado en la política general integral y bajo un enfoque aplicado de mejora continua y de gestión integral del riesgo:

	Infraestructura/Sistemas		
ELEMENTO DEL ALCANCE	**Infr. - S.I propios**	**Infr. – S.I del cliente**	
a. Prestación servicios de gestión de la información y sistemas de información (Software como servicios)	Permitido	Permitido	Portátiles
	No permitido	No permitido	iPad/Tablet
	No permitido	No permitido	Smartphone
	No permitido	No permitido	HDD externo
b. Administración delegada de infraestructura tecnológica, de hardware y de software, propia y/o de terceros	Permitido	Permitido	Portátiles
	No permitido	No permitido	iPad/Tablet
	No permitido	No permitido	Smartphone
	No permitido	No permitido	HDD externo
c. Ingeniería de software	Permitido	Permitido	Portátiles
	No permitido	No permitido	iPad/Tablet
	No permitido	No permitido	Smartphone
	No permitido	No permitido	HDD externo

1. Integra Web Prohíbe el almacenamiento y procesamiento de los datos.
2. Solo se autoriza el teletrabajo desde equipos de cómputo asignados por la compañía o aquellos autorizados por seguridad de la información.
3. La conexión se debe realizar desde sitios seguros, preferiblemente desde redes domésticas.
4. Al retirar el equipo de la compañía debe velar por su cuidado no exponiéndolo, ni abandonándolo en lugares públicos o privados, y en viajes debe siempre tenerlo consigo llevándolo como equipaje de mano y nunca almacenándolo en la bodega de carga.
5. Todo uso indebido de la información y del entorno físico es responsabilidad del empleado.
6. Todo ordenador o dispositivo móvil correspondiente estara bajo responsabilidad del empleado y cualquier uso indebido del mismo sera asumido por su empleado.
7. Los equipos autorizados para teletrabajo deberan pasar una validacion de seguridad de datos por la politica de proteccion de datos personales 1581 de 2012 con el fin de salvaguardar la informacion de todas las personas sea (clientes, proveedores, socios) de la empresa.
8. Integra Web implemento la modalidad de teletrabajo. Sin embargo, se mantiene la modalidad de trabajo hibrido con la finalidad de que los empleados de la empresa en los diferentes departamentos se pueda mantener el trabajo presencial o remoto según sea la opción más acorde para el empleado.
9. La organización no habilita acceso remoto directo a infraestructura interna, servidores locales ni redes corporativas desde ubicaciones externas.
10. El trabajo remoto se realiza exclusivamente mediante el uso de plataformas y servicios autorizados por la organización, operando sobre entornos en la nube o sistemas controlados.

6. Política de control de acceso

INTEGRA WEB, para la gestión integral en relación con su alcance respecto del teletrabajo, ha determinado los siguientes lineamientos bajo un enfoque aplicado de mejora continua y de gestión integral del riesgo:

- La asignación de derechos de acceso operará exclusivamente sobre una base contractual, de forma que será requisito la existencia de una relación contractual vigente entre las partes que determine específicamente que tipo de información va a estar en el dominio de quien suscribe el acuerdo, que acciones realizará sobre esa información y las razones de la misma.
- El ajuste y remoción de derechos de acceso será realizado inmediatamente finalice la relación contractual, y si es necesaria una etapa de transferencia, tales derechos de acceso estarán a cargo de quien recibe la información.
- Trimestralmente se realizarán actividades de revisión de derechos de acceso. De ser necesario aplicar algún tipo de ajuste, éstos serán realizados de forma inmediata.
- Ante cambios en contexto (requisitos y contratos) se realizarán actividades de revisión de derechos de acceso. De ser necesario aplicar algún tipo de ajuste, éstos serán realizados de forma inmediata.
- En el caso de medios externos y considerando su movilidad, el acceso incluirá responsabilidades sobre la posible pérdida y robo del medio externo.
- En el caso de archivo físico, especialmente de clientes, el acceso será dado en las instalaciones donde resida dicho archivo, sea en las instalaciones del cliente o en la organización (INTEGRA WEB) y no estará permitida la extracción parcial o total.
- La organización utilizará sistemas Wifi con no transmisión de su ID y solo se dará acceso a equipos de cómputo autorizados
- La organización podrá fortalecer los mecanismos de autenticación conforme a la evolución del análisis de riesgos y necesidades del negocio.
- La organizacion aplicará el principio de mínimo privilegio y segregación de funciones.

7. Política de escritorio limpio y de pantalla limpia.

INTEGRA WEB, para la para la gestión integral en relación con su alcance respecto a cómo las personas que realizan trabajos para la organización o en nombre de ella mantienen documentos y en general archivos en su espacio de trabajo y áreas relacionadas, ha determinado los siguientes lineamientos bajo un enfoque aplicado de mejora continua y de gestión integral del riesgo:

- En los equipos de cómputo, mantener únicamente el ícono de papelera de reciclaje, el de sistema (cuando éste sea el caso) y las aplicaciones que por funcionalidad o configuración determinada deban estar allí ubicados.
- En cuanto a archivos digitales y enlaces, si bien se pueden mantener (de forma temporal) algunos ejemplares en el escritorio, la carpeta de descargas y de documentos, éstos deben ser eliminados o archivados donde corresponde cuando finalice su procesamiento o sea necesario que la persona a cargo se retire de la estación de trabajo, así sea solo momentáneamente.
- Sobre los archivos físicos, solo se pueden mantener ejemplares en el escritorio mientras son procesados y deben ser archivados donde corresponde cuando finalice su procesamiento o sea necesario que la persona a cargo se retire de su sitio de trabajo, así sea solo momentáneamente.

- Para los archivos digitales y físicos, se deberán aplicar los principios archivísticos de procedencia y de orden original para asegurar una adecuada organización de los datos.
- Protección de contraseñas: Prohibir el almacenamiento de contraseñas escritas o documentos con información de acceso en el escritorio o en áreas de trabajo.
- Limpieza regular: Se establecen pautas para la limpieza regular de los escritorios y áreas de trabajo para asegurarse de que no haya documentos sensibles olvidados. Para los archivos digitales se mantiene la limpieza frecuente de datos en busca de no exponer informacion clasificada de los clientes

8. Política de copia de respaldo

INTEGRA WEB, para la gestión integral en relación con su alcance respecto a cómo asegura la disponibilidad e integridad de la información ante la ocurrencia de un incidente disruptivo del tipo pérdida o alteración de la información, ha determinado los siguientes lineamientos bajo un enfoque aplicado de mejora continua y de gestión integral del riesgo:

- El período mínimo de copias de seguridad es semanal.
- Cada persona que realice trabajos para la organización o en su nombre, con equipo de cómputo a su cargo, deberá realizar todas las actividades en One Drive y protocolos SSH para crear copia de seguridad de las actividades o tareas que realizan diariamente.
- Luego de cada copia de seguridad, se deben verificar los medios (soporte físico donde fue hecha la copia de seguridad) para asegurar su funcionamiento.
- Se pueden mezclar estrategias de copia incremental (agregando los archivos nuevos o mejorados) o total (copiando totalmente la información objetivo)
- Las copias de seguridad deben estar segmentadas, de forma que cada carpeta o elemento de organización contenga únicamente datos y documentos relacionados con una temática.
- Las copias estarán cifradas y almacenadas en ubicación segura y segregada.
- El medio donde se realiza la copia de seguridad debe estar ubicado en sitio externo a la oficina de INTEGRA WEB y resguardado ante una eventual pérdida de confidencialidad.
- El tiempo de retención de respaldos será definido conforme a requisitos legales y contractuales.

9. Política de continuidad del negocio y recuperación ante desastres

INTEGRA WEB, establece lineamientos para garantizar la continuidad de sus servicios y la recuperación oportuna ante eventos que puedan afectar la disponibilidad de la información o la prestación de sus servicios tecnológicos. La organización identifica como eventos disruptivos aquellos incidentes que puedan generar pérdida, alteración, indisponibilidad o acceso no autorizado a la información, así como fallas técnicas que impacten la operación del servicio.

Para mitigar estos riesgos, INTEGRA WEB implementa las siguientes medidas:

- Realización de copias de seguridad conforme a la política de respaldo vigente.
- Almacenamiento seguro de respaldos en ubicación segregada.
- Procedimientos documentados para la restauración de información.

- Monitoreo básico de disponibilidad de servicios críticos.
- Registro y gestión de incidentes que afecten la operación.

En caso de presentarse un incidente que comprometa la continuidad del servicio, se activarán las acciones necesarias para:

- Identificar y contener la causa del evento.
- Restaurar la operación utilizando los mecanismos de respaldo disponibles.
- Verificar la integridad de la información recuperada.
- Documentar el evento y definir acciones preventivas.

La organización evaluará periódicamente los riesgos que puedan afectar la continuidad del negocio y ajustará sus controles conforme al análisis realizado, al crecimiento del servicio y a los cambios tecnológicos o regulatorios.

10. Políticas para la transferencia de información

INTEGRA WEB, para la gestión integral en relación con su alcance respecto a cómo asegura la transferencia de información, ha determinado los siguientes lineamientos bajo un enfoque aplicado de mejora continua y de gestión integral del riesgo:

- Toda transferencia de información (interna o externa, desde o hacia la organización) debe estar identificada contemplando como mínimo conjunto de datos, remitente, destinatario, medio de transferencia y justificación de la misma. Para el caso de transferencias sucesivas, este elemento solo será identificado una única vez a menos que cambie el conjunto de datos.
- No está permitida la transferencia de información reservada o de carácter nacional fuera del territorio colombiano, lo cual incluye herramientas de acceso compartido.
- Toda transferencia de información debe generar su respectivo registro para asegurar trazabilidad.
- Ninguno de los usuarios de la empresa debería trabajar sobre el usuario administrador en su computador.
- Los usuarios normales (que no son administrador) deberian tener políticas restrictivas (ej. instalar o terminar aplicaciones).

11. Política de desarrollo seguro

INTEGRA WEB, para la gestión integral en relación con su alcance respecto a acciones de desarrollo de software, ha determinado los siguientes lineamientos bajo un enfoque aplicado de mejora continua y de gestión integral del riesgo:

- Todo desarrollo, mantenimiento, prueba, implementación o cambio de software debe incluir la definición o aplicación de requisitos de seguridad en el software.
- En el caso que el cliente no especifique requisitos de seguridad en el software, la organización establecera un estándar mínimo de requisitos de seguridad.
- Todo desarrollo de software realizado con terceros o personal interno de la organización deberá contar con un acuerdo de transferencia de derechos patrimoniales de autor hacia la organización.

- Todo desarrollo de software deberá incluir prácticas de desarrollo seguro, revisión de código, control de versiones y gestión de vulnerabilidades.
- La organización evaluará periódicamente la necesidad de fortalecer sus prácticas de desarrollo seguro conforme al análisis de riesgos y evolución tecnológica.

12. Política de seguridad de la información para relaciones con proveedores

INTEGRA WEB, para la gestión integral en relación con su alcance respecto a partes interesadas que le provean productos o servicios relacionados o con impacto en la información, sean éstos personas naturales o jurídicas, ha determinado los siguientes lineamientos bajo un enfoque aplicado de mejora continua y de gestión integral del riesgo:

- Todo acuerdo, contrato o similar, propuesta comercial, deberá incorporar requisitos de seguridad de la información que incluya como mínimo la adhesión a las políticas de seguridad de la información, cláusula de confidencialidad y la aplicación de las prácticas que estén relacionadas con su actividad.
- Todo acuerdo, contrato o similar, deberá incorporar requisitos de control y auditabilidad, según el riesgo, para poder conocer la aplicación de los lineamientos en seguridad de la información.
- Los proveedores que tengan acceso a información de la organización serán evaluados previamente en términos de riesgo y deberán cumplir requisitos de seguridad y confidencialidad establecidos contractualmente.

13. Política de seguridad de la información en gestión de proyectos

INTEGRA WEB, para la gestión integral en relación con su alcance sobre proyectos de cualquier tipo, ha determinado los siguientes lineamientos bajo un enfoque aplicado de mejora continua y de gestión integral del riesgo:

- Todo proyecto deberá incorporar requisitos de seguridad de la información que incluya como mínimo la adhesión a las políticas de seguridad de la información, cláusula de confidencialidad y la aplicación de las prácticas que estén relacionadas con su actividad.
- Los proyectos que la organización determine como de riesgo medio o alto, deberán incluir su propia identificación y análisis de riesgos, así como sus controles respectivos.
- Todo proyecto deberá incorporar mecanismos de seguimiento, medición y control para poder conocer la aplicación de los lineamientos generales y específicos en seguridad de la información.
- Todo equipo de cómputo, de propiedad de la organización o alquilado, será utilizado de forma exclusiva para los fines de la organización en horarios laborales (lunes a viernes de 8:00 am a 12:00 m y de 2:00 pm a 6:00 pm y sábados de 8:00 am a 12:00 pm), solo permitiendo elementos públicos de transmisión de música (YouTube) con auriculares y en horarios de descanso (lunes a viernes de 12:00 m a 2:00 pm y de 6:00 pm a 7:00 pm, los sábados de 12:00 pm a 1:00 pm) es permitido jugar videojuegos Open Sours y utilizar aplicaciones para entretenimiento desde el navegador.
- Con la nueva modalidad de trabajo hibrido se mantiene el horario laboral de lunes a viernes 8:00 am a 12:00 pm y 2:00 pm a 6:00 pm y sábados de 8:00 a 12:00 pm. Debido a la modalidad de trabajo, ya no aplican los tiempos para aplicaciones de entretenimiento en equipos empresariales.

Sin embargo, en los equipos personales se aplica el control de accesos para mantener por sesiones la información personal y laboral separada.

14. Política de instalación de software

INTEGRA WEB, para la gestión integral en relación con su alcance sobre instalación de software, incluyendo actualizaciones, ha determinado los siguientes lineamientos en un enfoque aplicado de mejora continua y de gestión integral del riesgo:

- Toda instalación de software, incluidas actualizaciones, será realizada de forma manual por personal explícitamente autorizado por la organización.
- Antes de realizar cualquier instalación, se deberán realizar pruebas para determinar el nivel de riesgo asociado a ese software a ser instalado.
- Todo equipo de cómputo, de propiedad de la organización o alquilado, deberá tener deshabilitada la opción de instalación de software.

15. Política de gestión de licencias

- Los equipos que no sean de propiedad de integra web y se les permita tener información de la organización es responsabilidad del funcionario o contratista contar con el software de su dispositivo debidamente licenciado.
- Se evalua regularmente la necesidad de actualizaciones de software para garantizar que la organización utilice versiones seguras y compatibles.

16. Política de equipos desatendidos

INTEGRA WEB, para la gestión integral en relación con su alcance en los equipos desatendidos, ha determinado los siguientes lineamientos en un enfoque aplicado de mejora continua y de gestión integral del riesgo:

- - Los equipos de cómputo y móviles deben tener contraseña y se debe activar su protección a los dos minutos de inactividad.
- Se mantendra un inventario actualizado de todos los equipos desatendidos, incluyendo su ubicación, función y responsable de supervisión.
- Todos los equipos desatendidos deben configurarse siguiendo las mejores prácticas de seguridad y actualizarse regularmente con parches de seguridad y actualizaciones de software.
- Se establecen medidas de control de acceso para restringir el acceso no autorizado a los equipos desatendidos. Esto incluye la autenticación segura y el principio de "menos privilegios".

17. Política de protección de datos

INTEGRA WEB, para la gestión integral en relación con su alcance en los datos de carácter personal, serán sometidos a los fines establecidos conforme a la ley 1581 de 2012 y sus decretos reglamentarios, ha determinado los siguientes lineamientos en un enfoque aplicado de mejora continua y de gestión integral del riesgo:

- Cuando los datos sobre los cuales se esté brindando acceso sean de carácter personal, se deberá adicionalmente suscribir un acuerdo de transferencia y responsabilidad de datos personales.
- Sin importar los posibles derechos de acceso aplicables, está prohibida la copia, parcial o total, de datos, documentos y demás relacionados.
- Toda información manejada por la organización será para uso exclusivo de la misma.
- La utilización, copia, impresión, retención, divulgación, reenvío o cualquier acción no autorizada a la información de carácter personal será sancionada legalmente.
- En caso de presentarse un incidente que comprometa datos personales, la organización activará el procedimiento interno de gestión de incidentes, documentará el evento y adoptará las medidas correctivas correspondientes.
- La organización revisará periódicamente sus controles de protección de datos personales como parte del proceso de mejora continua del sistema de gestión de seguridad de la información.

Versión	Fecha	Numerales	Descripción del documento
01	01/02/2020	Todos	Creación del documento
02	13/03/2020	Políticas móviles, tele trabajo y criptograficas.	Se complementaron las políticas con el contexto actual
03	16/03/2021	Políticas SGSI	Se modificó las políticas de un sistema de gestión Integral donde se involucraba ISO 9001 y la ISO 27001.
04	30/05/2023	Versionamiento	Se agregó tabla de versiones.
05	25/10/2023	Actualizacion Politica Integral	Se actualiza la politica integral a nivel general del SGSI
06	08/05/2024	Actualización Política de desarrollo seguro	Se actualiza la política integral anexando mejoras para el desarrollo seguro
07	20/02/2026	Actualizacion Politica Integral	Se actualiza la politica integral a nivel general del SGSI

FIRMA DE APROBACIÓN

CAMILO ANDRÉS ECHEVERRY

Representante legal