En **PROYECTOS Y GESTION DEL DESARROLLO S.A.S.,** es de mucha importancia el aseguramiento de los datos personales e información y por eso ha venido desarrollando su modelo de seguridad de la información, ciberseguridad y los datos, adoptando buenas prácticas en cuanto a la gestión y administración de los mismos.

Alcance / Aplicabilidad

Esta política aplica a toda la empresa, sus funcionarios, terceros, proveedores y clientes. La presente política aplicará para el manejo de la información y datos personales que sea utilizada y/o se encuentre en las bases de datos que contengan activos de información de **PROYECTOS Y GESTION DEL DESARROLLO S.A.S**, quien en lo sucesivo se denominará "**PROYECTOS Y GESTION DEL DESARROLLO S.A.S**", quien actúa en calidad de Responsable del tratamiento de la Información, de esos datos personales y los activos que contengan información de la organización a nivel físico, digital, aplicaciones y plataformas tecnológicas tanto en la red interna como las que interactúan con internet.

Objetivos de Seguridad

1. Comunicar y hacer toma de conciencia de la gestión y cumplimiento de políticas, normas y procedimientos de seguridad.

2. Mantener los controles de acceso físico y lógico, Seguridad Local, Gestión de Actualizaciones de Seguridad funcionales y que puedan garantizar la integridad de la información.

3. Monitoreo y protección de las bases de datos, gestionar los Incidentes de Seguridad y ciberseguridad, en caso de presentarse.

4. Mantener la capacitación y concienciación del personal en temas de seguridad de la información, ciberseguridad y los datos mediante el programa de capacitación.

5. Gestión con terceras partes, proveedores, outsourcing y Control en la transferencia de información.

6. Identificar, Controlar y Monitorear los Riesgos relacionados con la Operación de La Empresa en cuanto a la Seguridad de la Información, Ciberseguridad y los Activos que contienen datos e información.

7. Asegurar la Confidencialidad, Integridad y Disponibilidad de los activos de información a través de la ejecución de políticas, gestión de riesgo y aseguramiento informático de plataformas IT.
8. Definir e implementar controles informáticos robustos para mitigar ataques cibernéticos conocidos, a los que se encuentran expuestas las aplicaciones y plataformas IT de la organización.

9. Gestionar la vulnerabilidad técnica y tratar el riesgo asociado a través de los análisis de vulnerabilidades sobre las plataformas IT.

Disposiciones normativas

De conformidad con lo establecido por la legislación vigente en materia de Habeas Data, específicamente la Ley Estatutaria 1581 de 2012, Decreto 1377 de 2013, Decreto Único Reglamentario 1074 de 2015, en su capitulo 26, en cumplimiento de lo dispuesto en la circular 002 de 03 Noviembre de 2015 y lo modificado en Dec. 1759 del 08 de Nov. de 2016, PROYECTOS Y GESTION DEL DESARROLLO S.A.S Informa sus políticas de tratamiento de la información y los datos recolectados y los mecanismos adoptados para su protección.

El artículo 15 de la Constitución de la República de Colombia establece que cualquier persona tiene derecho a conocer, actualizar y rectificar los datos personales que existan sobre ella en banco de datos o archivos de entidades públicas o privadas. Igualmente, ordena a quienes tengan datos personales de terceros respetar los derechos y garantía previstos en la Constitución cuando se recolecta, trata y circula esa clase de información.

La Ley Estatutaria 1581 del 17 de octubre de 2012 establece las condiciones mínimas para realizar el tratamiento legítimo de los datos personales de los clientes, empleados y cualquier otra persona natural. El literal k) del artículo 18 de dicha ley obliga a los responsables del tratamiento de datos personales a adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la citada ley y en especial, para la atención de consultas y reclamos.

De conformidad con la ley 1273 de 2009 incurre en el delito de violación de datos personales quien "sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes".

Así mismo y en virtud de los términos del sector de las Infraestructuras del mercado financiero, establece la política de Ciberseguridad, la cual se encuentra fundamentada en los marcos de referencia ISO 27001 e ISO 27032.

PROYECTOS Y GESTION DEL DESARROLLO S.A.S está comprometida con el respeto y garantía de los derechos de sus empleados, contratistas, proveedores y terceros en general. Por eso adopta el siguiente manual de políticas y procedimientos de tratamiento de Información, de obligatoria aplicación en todas las actividades que involucre, total o parcialmente, la recolección, el almacenamiento, el uso, la circulación y transferencia de esa información y datos siendo de obligatorio y estricto cumplimiento para **PROYECTOS Y GESTION DEL DESARROLLO S.A.S,** en calidad de responsable, así como todos los terceros que obran en nombre de la misma o que sin actuar en nombre de **P Y G DELDESARROLLO S.A.S.** tratan datos personales por disposición de ésta como encargados.

Tanto el responsable, como los encargados, entiéndase, empleados, contratistas y terceros deben observar y respetar estas políticas en el cumplimiento de sus funciones y/ o actividades aún después de terminados los vínculos legales, comerciales, laborales o de cualquier índole. De igual manera, deberán guardar estricta confidencialidad en relación con los datos tratados.

Cualquier incumplimiento de las obligaciones y en general, de las políticas contenidas en este documento debe ser reportado a través de la Línea Telefónica No. **6554220**

Definiciones

Para efectos de la interpretación y aplicación de ésta política deben tenerse en cuenta los siguientes conceptos:

Autorización: Consentimiento previo, expreso e informado del titular del dato para llevar a cabo el tratamiento de su información personal.

Dato personal: Cualquier información que directa o indirectamente se refiere a una persona natural y que permite identificarla. Son algunos ejemplos de datos personales los siguientes: nombre, número de identificación ciudadana, dirección física, dirección de correo electrónico, número telefónico, estado civil, datos de salud, huella dactilar, salario, bienes, estados financieros, etc.

Dato personal sensible: Información que afecta la intimidad de la persona o cuyo uso indebido puede generar su discriminación, tales como por ejemplo 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 (huellas dactilares, fotos, videos)

Dato personal público: Es el dato calificado como tal por ley o la Constitución Política o el que no sea privado, semiprivado o sensible. Son 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, los datos contenidos en el RUNT o los datos contenidos en el registro público mercantil de las Cámaras de Comercio. 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.

Estos datos pueden ser obtenidos y ofrecidos sin reserva alguna y sin importar si hacen alusión a información general, privada o personal.

Dato personal privado. Es el dato que por su naturaleza íntima o reservada sólo es relevante para la persona titular del dato. Ejemplos:

libros de los comerciantes (contabilidad), información extraída a partir de la inspección del domicilio, número telefónico siempre y cuando no se encuentre en bases públicas o el salario.

Dato personal semiprivado. Es semiprivado el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como, entre otros, el dato referente al cumplimiento o incumplimiento de las obligaciones financieras o los datos relativos a las relaciones con las entidades de la seguridad social.

Encargado del tratamiento: Persona que realiza el tratamiento de datos por cuenta del Responsable del Tratamiento.

Reclamo: Solicitud del titular del dato o las personas autorizadas por éste o por la ley para corregir, actualizar o suprimir sus datos personales o para revocar la autorización en los casos establecidos en la ley.

Responsable del tratamiento: Persona que decide sobre la recolección de datos y fines del tratamiento, entre otras. Puede ser, a título de ejemplo, la empresa dueña de las bases de datos o sistema de información que contiene datos personales.

Titular del dato: Es la persona natural cuyos datos personales sean objeto de tratamiento.

Tratamiento: Cualquier operación o conjunto de operaciones sobre datos personales como, entre otros, la recolección, el almacenamiento, el uso, la circulación o supresión de esa clase de información. Transferencia: Envío de datos personales que realiza el Responsable o el Encargado desde Colombia a un Responsable que se encuentra dentro (transferencia nacional) o fuera del país (transferencia internacional).

Transmisión: Tratamiento de datos personales que implica la comunicación de los mismos dentro (transmisión nacional) o fuera de Colombia (transmisión internacional) y que tiene por objeto la realización de un tratamiento por el Encargado por cuenta del Responsable.

Menores: hace referencia los menores de 18 años, y corresponde a los
Niños Niñas y Adolescentes.

Antivirus: Software que escanea un dispositivo o una red para detectar amenazas de seguridad, alertarlo y neutralizar códigos maliciosos.

Autenticador: Un método de cómo un usuario puede probar su identidad a un sistema. Puede ser una contraseña, una huella digital, un escaneo facial.

Lista negra: Una lista de correos electrónicos u otros proveedores de servicios que difunden mensajes de spam. Las listas negras ayudan a los usuarios y empresas a evitar la avalancha de mensajes no deseados.

Copia de seguridad: Una copia de los datos físicos o virtuales para que, en caso de que se eliminen o se pierdan, el usuario pueda recuperarlos fácilmente. Funciona como parte de un plan de prevención de pérdida de datos.

Código cerrado: Una tecnología patentada cuyo copyright oculta su código fuente y prohíbe su distribución o modificación. Ejemplos de software comercial de código cerrado son Skype, Java, Opera.

Prevención de pérdida de datos (DLP): El complejo de medidas de seguridad relacionadas con la detección y prevención de la pérdida de datos y los ciberataques. DLP está incluido en la política de la organización, pero las personas también deben usar esta estrategia para mantener todos los datos seguros durante un ataque de ransomware o malware.

Cifrado de datos: Una forma de proteger la información privada codificándola para que ningún tercero pueda verla o acceder a ella. Para leer el archivo codificado (cifrado), debes decodificarlo utilizando una clave de descifrado.

Protección de datos: Un conjunto de métodos destinados a proteger la información privada para que no caiga en las manos equivocadas.

Exploit: Un punto débil en un sistema informático, que puede usarse para atacar este sistema.

Cortafuegos: Un sistema de seguridad de red que filtra el tráfico entrante y saliente no autorizado.

Autenticador de grupo: Se utiliza para permitir el acceso a datos o funciones específicos que pueden ser compartidos por todos los miembros de un grupo en particular.

Honeypot: Una técnica que tiene como objetivo distraer a los piratas informáticos con un objetivo falso (una computadora o datos) y hacer que lo persigan en lugar del real. Ayuda a asegurar un objetivo de alto valor y observar las principales técnicas de los piratas informáticos para aprender de ellos.

Dirección IP: Una dirección que identifica la conexión entre tu computadora y el proveedor de red. Tu computadora puede tener varias direcciones IP dependiendo de la cantidad de redes a las que se conecta. Además, varias computadoras pueden tener una dirección IP si están conectadas al mismo proveedor en la misma área, como en cafés o en casa.

Verificación de identidad: Un conjunto de acciones (una contraseña, una huella digital o un escaneo facial) diseñadas para verificar la identidad de una persona.

Plan de respuesta a incidentes: Un conjunto de medidas que se deben tomar en caso de un ciberataque para reducir los daños del ataque. Es parte de la gestión de respuesta a incidentes.

Amenaza interna: Una amenaza a la integridad de los datos de la empresa que proviene de alguien dentro de la organización, generalmente un empleado u otra persona interna.

Código abierto: Un tipo de tecnología libre cuyo derecho de autor permite utilizar su código fuente para diferentes propósitos, como estudiar, modificar, distribuir. Ejemplos de código de fuente abierta son Bitcoin, Mozilla Firefox, Joomla, WordPress.

Parche: Una actualización regular del sistema que está diseñada para cubrir los errores de seguridad que se han descubierto.

ReCAPTCHA: Un sistema inventado por Google que utiliza una prueba de Turing para establecer si un usuario es un humano o un robot. Los sitios web lo utilizan para evitar que los bots envíen spam.

Shadow IT: Denota cualquier sistema de TI que se haya implementado en la organización sin la autorización del departamento de TI. El hardware y el software no autorizados pueden convertirse en un punto de entrada para los ciberataques. Las aplicaciones en la nube son uno de los tipos de TI en la sombra más inseguros.

Red privada virtual (VPN): Tecnología que extiende una red privada y todo su cifrado, seguridad y funcionalidad a través de una red pública. Con él, los usuarios pueden enviar y recibir mensajes como si estuvieran conectados a una red privada.

Prueba de lápiz: Un medio de evaluación de la seguridad en el que expertos en seguridad y ataques realizan herramientas automatizadas y explotaciones manuales. Esta es una forma avanzada de evaluación de la seguridad que solo deben utilizar los entornos con una infraestructura de seguridad madura.
Una prueba de penetración utilizará las mismas herramientas, técnicas y metodologías que los piratas informáticos criminales y, por lo tanto, puede causar tiempo de inactividad y daños al sistema. Sin embargo, tales evaluaciones pueden ayudar a proteger una red al descubrir fallas que no son visibles para las herramientas automatizadas basadas en conceptos de ataques humanos (es decir, ingeniería social) o físicos.

IDS (Sistema de detección de intrusiones): Una herramienta de seguridad que intenta detectar la presencia de intrusos o la ocurrencia de violaciones de seguridad para notificar a los administradores, permitir un registro más detallado o enfocado o incluso desencadenar una respuesta como desconectar una sesión o bloquear una IP. habla a. Un IDS se considera una herramienta de seguridad más pasiva, ya que detecta compromisos después de que ya están ocurriendo en lugar de evitar que tengan éxito.

DLP (Prevención de pérdida de datos): Una colección de mecanismos de seguridad que tienen como objetivo prevenir la ocurrencia de pérdida y / o fuga de datos. La pérdida de datos ocurre cuando un dispositivo de almacenamiento se pierde o es robado, mientras que la fuga de datos ocurre cuando entidades no autorizadas poseen copias de los datos. En ambos casos, los datos son accesibles para quienes no deberían tener acceso.
DLP tiene como objetivo prevenir tales ocurrencias a través de diversas técnicas, como controles estrictos de acceso a los recursos, bloquear el uso de archivos adjuntos de correo electrónico, evitar el intercambio de archivos de red a sistemas externos, bloquear cortar y pegar, deshabilitar el uso de redes sociales y cifrar los datos almacenados.

Esquemas para el manejo, tratamiento y seguridad de la información y los datos

PROYECTOS Y GESTION DEL DESARROLLO S.A.S cuenta con infraestructura administrativa para asegurar la debida atención de requerimientos, peticiones, consultas, quejas y reclamos relativos a protección de datos, con el fin de garantizar el ejercicio de los derechos contenidos en la Constitución y la ley, especialmente el derecho a conocer, actualizar, rectificar y suprimir información personal; así como el derecho a revocar el consentimiento otorgado para el tratamiento de datos personales.

Igualmente, **PROYECTOS Y GESTION DEL DESARROLLO S.A.S** cuenta con procedimientos y herramientas para la autenticación de sus titulares como mecanismo de validación de la identidad del titular como única persona[1] que puede conocer, actualizar, rectificar y suprimir información personal a través de los canales de servicio a saber:

[1] Para el caso de los menores de edad se solicitará a su representante o acudiente la presentación del documento que acredite el parentesco o relación que lo vincule como representante legal del menor.

1. Correo Electrónico: **contacto@pygdeldesarrollo.com**
2. Línea telefónicas: **+57 5 6554220**
3. Oficina de Atención: **KRA. 3RA. NO.46-57 EDIFICIO LAGUNA 46 OFICINA 1401 - MARBELLA – CARTAGENA**
4. Pagina web: **www.pygdeldesarrollo.com**

Todos los canales anteriores cuentan con personal capacitado para el desempeño de sus funciones e igualmente con los sistemas de control necesarios para que las novedades de información personal que los titulares soliciten queden documentadas y puedan ser objeto de trazabilidad.

Sólo se enviarán los datos personales las siguientes personas:

Al titular del dato, sus causahabientes o sus representantes legales.
A las personas autorizadas por el titular del dato.
A las personas autorizadas por orden judicial o legal.

En este último caso, de conformidad con el pronunciamiento de la Corte Constitucional, se procederá de la siguiente manera:
En primer lugar, la entidad pública o administrativa debe justificar su solicitud indicando el vínculo entre la necesidad de obtener el dato y el cumplimiento de sus funciones constitucionales o legales.

En segundo lugar, con la entrega de la información se le informará a la entidad pública o administrativa que debe cumplir los deberes y obligaciones que le impone la Ley 1581 de 2012 como Responsable del tratamiento. La entidad administrativa receptora debe cumplir con las obligaciones de protección y garantía que se derivan de la citada ley, en especial la observancia de los principios de finalidad, uso legítimo, circulación restringida, confidencialidad y seguridad.

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 en la ley o por el titular del dato.

Derechos y deberes de los titulares de la información

PROYECTOS Y GESTION DEL DESARROLLO S.A.S se compromete a respetar y garantizar los siguientes derechos de los titulares de los datos:

- Conocer, actualizar y rectificar los datos personales. Para el efecto es necesario establecer previamente la identificación de la persona para evitar que terceros no autorizados accedan a los datos del titular del dato.
- Obtener copia de la autorización otorgada por éstos en calidad de titulares de los datos.
- Conocer el uso que **PROYECTOS Y GESTION DEL DESARROLLO S.A.S** ha dado a los datos personales del titular.
- Consultar sus datos personales y hacer reclamos para salvaguardar su derecho a la protección de sus datos personales siguiendo las pautas establecidas en la ley y en la presente política.
- Supresión del dato personal cuando la Superintendencia de Industria y Comercio haya determinado que en el tratamiento por parte de **PROYECTOS Y GESTION DEL DESARROLLO S.A.S** se ha incurrido en conductas contrarias a la ley 1581 de 2012 o a la Constitución.
- Acceder en forma gratuita a sus datos personales, la información solicitada por el titular podrá ser suministrada por cualquier medio, incluyendo los electrónicos, según lo requiera

el titular. La información deberá ser de fácil lectura y deberá corresponder en un todo a aquella que repose en las bases de datos o archivos de **P Y G DEL DESARROLLO S.A.S.**

En ningún caso el titular del dato podrá revocar la autorización y solicitar la supresión del dato, cuando exista un deber legal o contractual que le imponga el deber de permanecer en la base de datos o archivo del Responsable o Encargado.

Cuando **PROYECTOS Y GESTION DEL DESARROLLO S.A.S** recolecte datos personales sensibles, el titular tiene la facultad de responder las preguntas que versen sobre este tipo de datos.

Los datos personales sensibles serán mantenidos y tratados con estricta seguridad y confidencialidad para los fines relacionados con la actividad económica de la empresa, conforme a la legislación y reglamentación aplicable.

PROYECTOS Y GESTION DEL DESARROLLO S.A.S en cumplimiento de las normas sobre Protección de Datos Personales, señala el procedimiento y requisitos mínimos para el ejercicio de los derechos de los titulares de la información.

PROCEDIMIENTOS y GENERALIDADES:

Los titulares de datos o sus representantes podrán consultar la información personal del titular que repose en las bases de datos de **PROYECTOS Y GESTION DEL DESARROLLO S.A.S** Los derechos de los niños, niñas o adolescentes se ejercerán por las personas que estén facultadas para representarlos.

El artículo 9 del Decreto 1377 de 2013 señala en su inciso segundo que "*La solicitud de supresión de la información y la revocatoria de la autorización no procederán cuando el titular tenga un deber legal o contractual de permanecer en la base de datos*.", el cual aplica entre otros a los afiliados al Sistema General de Seguridad Social en Salud, pues ellos están en la obligación de estar afiliados al Sistema.

En aras de facilitar a sus titulares el acceso a su propia información, **PROYECTOS Y GESTION DEL DESARROLLO S.A.S** ha establecido canales para realizar consultas y novedades tales como:

1. Consulta y actualización de datos personales.
2. Verificar estado y tipo de información personal usado en base de datos.
3. Existencia y estado de autorización para uso de sus datos.

Dichos canales son:

1. Correo Electrónico: **contacto@pygdeldesarrollo.com**
2. Línea telefónicas: **+57 5 6554220**
3. Oficina de Atención: **KRA. 3RA. NO.46-57 EDIFICIO LAGUNA 46 OFICINA 1401 - MARBELLA – CARTAGENA**
4. Pagina web: **www.pygdeldesarrollo.com**

En caso de consultas adicionales, o que se considere que la información debe ser objeto de corrección, actualización o supresión, o cuando se advierta el presunto incumplimiento de cualquiera de los deberes

en la protección de los datos, el titular o su representante podrán presentar un reclamo ante **PROYECTOS Y GESTION DEL DESARROLLO S.A.S.**

Vías para la presentación de consultas y reclamos:

Dado que toda consulta o reclamo presentado por el titular debe contar con la evidencia de su trámite, **PROYECTOS Y GESTION DEL DESARROLLO S.A.S** Establece como vía para su presentación la forma escrita en carta original radicada en la oficina de atención de **PROYECTOS Y GESTION DEL DESARROLLO S.A.S** El área responsable de su trámite será el Área Administrativa de **PROYECTOS Y GESTION DEL DESARROLLO S.A.S.**

Cuando se presente en la oficina a radicar su consulta o reclamo puede solicitar el radicado o comunicarse en dos días hábiles, con su número de seguimiento y saber el estado de su trámite. Para el caso de contratistas, proveedores y prestadores persona natural se puede hacer mediante correo electrónico dirigido a la siguiente dirección: contacto@pygdeldesarrollo.com

Contenido de la consulta o reclamo:

La solicitud debe estar dirigida a **PROYECTOS Y GESTION DEL DESARROLLO S.A.S** y debe contener como mínimo los siguientes datos:

1. Nombres y apellidos del titular.
2. Número de identificación del titular.
3. Datos de localización del titular.
4. Descripción de los hechos que dan lugar a la consulta o reclamo.
5. Documentos que considere soportan su consulta o reclamo.
6. Medio por el cual desea recibir respuesta
7. Nombre del peticionario, el cual, si es diferente al titular, debe adjuntar los documentos que le permitan actuar en su nombre.
8. Firma del peticionario.

Tiempos para el trámite de una consulta o reclamo

Las consultas serán atendidas en un término máximo de diez (10) días hábiles contados a partir del día siguiente a la fecha de recibo de la misma. Cuando no fuere posible atender la consulta dentro de dicho término, se informará al titular o interesado los motivos de la demora y señalando la fecha en que se atenderá su consulta, la cual no será superior a los cinco (5) días hábiles siguientes al vencimiento del primer término.

Para los reclamos, si alguno resulta incompleto, se requerirá al titular o interesado dentro de los cinco (5) días siguientes a la recepción del mismo para que subsane las falencias identificadas. Transcurridos dos (2) meses desde la fecha del requerimiento, sin que el titular o interesado presente la información requerida, se entenderá que ha desistido del reclamo.

Sí, **PROYECTOS Y GESTION DEL DESARROLLO S.A.S** no es la entidad competente para resolver un reclamo, dará traslado del mismo a quien corresponda en un término máximo de dos (2) días hábiles si

el nuevo responsable es identificable e informará de la situación al interesado para que pueda hacer seguimiento o identifique claramente la entidad a la cual debe dirigirse.

Una vez **PROYECTOS Y GESTION DEL DESARROLLO S.A.S** Haya recibido el reclamo completo, se marcará el caso en las bases de datos con una leyenda "Reclamo en trámite" y el motivo del mismo, máximo en dos (2) días hábiles y así semantendrá hasta definir la respuesta.

Inconformidad con la respuesta de la consulta o reclamo:

Si no hay conformidad con la respuesta emitida puede solicitar reconsideración directamente a **PROYECTOS Y GESTION DEL DESARROLLO S.A.S**, cumpliendo nuevamente con los pasos definidos en este procedimiento.

De acuerdo con lo dispuesto en el artículo 16 de la Ley 1581 de 2012, el titular o interesado sólo podrá elevar queja ante la Superintendencia de Industria y Comercio una vez haya agotado el trámite de consulta o reclamo ante **P Y G DEL DESARROLLO S.A.S.**

Costos del trámite:
El Titular podrá consultar de forma gratuita sus datos personales al menos una vez cada mes calendario o cada vez que existan modificaciones sustanciales de las políticas de tratamiento de la información que motiven nuevas consultas.
Para consultas cuya periodicidad sea mayor a una por cada mes calendario, **PROYECTOS Y GESTION DEL DESARROLLO S.A.S** Podrá cobrar al Titular los gastos de envío, reproducción o certificación de documentos.

Deberes de PROYECTOS Y GESTION DEL DESARROLLO S.A.S:

- Solicitar y conservar, en las condiciones previstas en esta política, copia o grabación de la respectiva autorización otorgada por el titular.
- Informar de manera clara y suficiente a los titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada.
- Garantizar al titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data, es decir, conocer, actualizar o rectificar sus datos personales.
- Informar a solicitud del titular sobre el uso dado a sus datos personales.
- Tramitar las consultas y reclamos formulados en los términos señalados en la presente política.
- Observar los principios de veracidad, calidad, seguridad y confidencialidad en los términos establecidos en la presente política.
- Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
- Actualizar la información cuando sea necesario.
- Rectificar los datos personales cuando ello sea procedente.
- Suministrar al Encargado del tratamiento únicamente los datos personales que está autorizado a suministrar a terceros.
- Garantizar que la información que se suministre al Encargado del tratamiento sea veraz, completa, exacta, actualizada, comprobable y comprensible.
- Comunicar de forma oportuna al Encargado del tratamiento todas las novedades respecto de los datos que previamente le haya suministrado.
- Exigir al Encargado del tratamiento, en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del titular.

- Informar al Encargado del tratamiento cuando determinada información se encuentre en discusión por parte del titular.

Sí **PROYECTOS Y GESTION DEL DESARROLLO S.A.S** Realiza el tratamiento de datos en nombre de otra entidad u organización (Responsable del tratamiento) deberá cumplir los siguientes deberes:

- Verificar que el Responsable del tratamiento esté autorizado para suministrar a **PROYECTOS Y GESTION DEL DESARROLLO S.A.S** los datos personales que tratará como Encargado.
- 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.
- 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 presente política.
- Registrar en la base de datos las leyendas "reclamo en trámite" en la forma en que se establece en la presente política.
- 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 Superintendencia de Industria y Comercio.
- Permitir el acceso a la información únicamente a las personas autorizadas por el titular o facultadas por la ley para dicho efecto.
- Informar a la Superintendencia de Industria y Comercio 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 Superintendencia de Industria y Comercio.

Tratamiento especial de ciertos datos personales

PROYECTOS Y GESTION DEL DESARROLLO S.A.S Accede a la información sensible del titular para garantizar su derecho a la salud, frente a esta información **PROYECTOS Y GESTION DEL DESARROLLO S.A.S** Identifica los datos sensibles y los datos de los niños, niñas y adolescentes (menores) que eventualmente recolecten o almacenen y sobre estos:

- Garantiza el especial cuidado y responsabilidad reforzada en el tratamiento de estos datos, lo que se traduce en una exigencia mayor en términos de cumplimiento de los principios y los deberes de protección.
- Cuenta con niveles de seguridad de esa información.
- Ha implementado restricciones de acceso y uso a esta información.

Los datos sensibles relacionados con el estado de salud del titular se consideran parte de la Historia Clínica y serán manejados bajo la reserva legal.

PROYECTOS Y GESTION DEL DESARROLLO S.A.S Cuenta con normas y procedimientos que garantizan que solamente idóneo manejen esta información.

PROYECTOS Y GESTION DEL DESARROLLO S.A.S Cuenta con medidas especiales de índole técnica y administrativas necesarias que garanticen la seguridad de los datos sensibles y eviten su

alteración, pérdida, tratamiento o acceso no autorizado a la información, tales como medidas de seguridad dispuestos para el tratamiento de los mismos.

Tratamiento de la información, niveles y medidas de Seguridad.

PROYECTOS Y GESTION DEL DESARROLLO S.A.S., podrá conservar los datos personales de los titulares de la información en bases de datos ubicadas en Colombia o en el extranjero, cumpliendo con la finalidad autorizada por el titular de los datos, realizando sus mayores esfuerzos para mantener la información de manera segura, salvaguardando su integridad, veracidad y confidencialidad.

PROYECTOS Y GESTION DEL DESARROLLO S.A.S. cuenta con políticas de Seguridad de la Información y los Datos, donde uno de los objetivos es lograr que la información mantenga su disponibilidad, integridad y confidencialidad, también apoyar a **PROYECTOS Y GESTION DEL DESARROLLO S.A.S** en el cumplimiento de sus obligaciones normativas de protección de la información y los datos, tanto de orden legal, como interno. Adicionalmente, se aplican recomendaciones y buenas prácticas de seguridad de estándares internacionales y requisitos de seguridad en concordancia con legislación Colombiana.

La gestión de la seguridad de la información, ciberseguridad y los datos, está basada en las siguientes medidas y controles:

- **Gestión de cumplimiento de políticas, normas y procedimientos de seguridad**
- **Controles de acceso físico y lógico**
- **Seguridad Local**
- **Gestión de Actualizaciones de Seguridad**
- **Monitoreo y protección de las bases de datos**
- **Gestión de Incidentes de Seguridad**
- **Capacitación y Concienciación - Simulacros**
- **Auditorias**
- **Gestión con terceras partes, proveedores, outsourcing**
- **Control en la transferencia de información**.
- **Monitoreo y seguimiento de riesgos en Matriz de Riesgos**
- **Identificar, Controlar y Monitorear los Riesgos relacionados con la Operación de La Empresa en cuanto a la Seguridad de la Información, Ciberseguridad y los Activos que contienen datos e información.**
- **Asegurar la Confidencialidad, Integridad y Disponibilidad de los activos de información a través de la ejecución de políticas, gestión de riesgo y aseguramiento informático de plataformas IT.**
- **Definir e implementar controles informáticos robustos para mitigar ataques cibernéticos conocidos, a los que se encuentran expuestas las aplicaciones y plataformas IT de la organización.**
- **Gestionar la vulnerabilidad técnica y tratar el riesgo asociado a través de los análisis de vulnerabilidades sobre las plataformas IT.**

Todas las medidas de seguridad que tiene **PROYECTOS Y GESTION DEL DESARROLLO S.A.S** se enfocan a la protección de la información y los datos. Estas medidas permiten tener el control sobre qué empleados acceden, modifican o cambian, borran, adulteran, eliminan la información y/o datos personales, de acuerdo a los perfiles asignados. **PROYECTOS Y GESTION DEL DESARROLLO S.A.S** clasifica los datos de acuerdo con su criticidad y establece las medidas de seguridad para asegurar su protección.

Frente a la protección de datos personales y/o sensibles **PROYECTOS Y GESTION DEL DESARROLLO S.A.S** procurará establecer los niveles y medidas de seguridad adecuados que garanticen de una manera razonable la confidencialidad, integridad y disponibilidad de los datos personales conforme lo establezca la Superintendencia de Industria y Comercio. Dichas medidas de seguridad establecidas serán de estricto cumplimiento para **PROYECTOS Y GESTION DEL DESARROLLO S.A.S** como para los encargados para el tratamiento de los datos.

PROYECTOS Y GESTION DEL DESARROLLO S.A.S podrá transferir o transmitir, todos o parte de los datos personales de los titulares de la información a entidades autorizadas de acuerdo con la legislación colombiana para la realización de actividades y prestación de servicios, así como a sus empleados, contratistas, proveedores y/o asesores, únicamente para efectos de la prestación de servicios del objeto social de la respectiva empresa con la que se tenga vinculo contractual.

Transferencia internacional de datos personales

Cuando se envíen o transfieran datos a otro país será imprescindible contar con la autorización del titular de la información que es objeto de transferencia. Salvo que la ley diga lo contrario, es presupuesto necesario la existencia de dicha autorización para efectuar la circulación internacional de datos. En este sentido, antes de enviar datos personales a otro país, el responsable deberá verificar que se cuenta con la autorización previa, expresa e inequívoca del titular que permita trasmitir sus datos personales.

Dicha transferencia de los datos personales se realiza únicamente a terceros con quienes **PROYECTOS Y GESTION DEL DESARROLLO S.A.S** tenga vínculo contractual, comercial y/o jurídico, en los casos en que el titular solicite los servicios en países en los cuales existe presencia de **PROYECTOS Y GESTION DEL DESARROLLO S.A.S** y de acuerdo al clausulado y/o al plan de beneficios, previa aprobación del responsable de la base de datos.

Aviso de Privacidad

PROYECTOS Y GESTION DEL DESARROLLO S.A.S informa que el aviso de privacidad de tratamiento de sus datos personales puede consultarlo en la pagina web www.pygdeldesarrollo.com o haciendo una solicitud al correo electrónico: **contacto@pygdeldesarrollo.com**

Modificación y/o actualización de la política de protección de datos y manejo de información

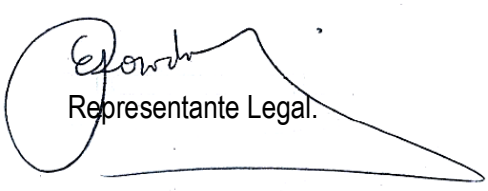
Cualquier cambio sustancial en las políticas de tratamiento, se comunicará de forma oportuna a los titulares de los datos a través de los medios habituales de contacto establecidos por la empresa.

Las comunicaciones se enviaran como mínimo diez (10) antes de implementar las nuevas políticas y/o actualización sustancial de la misma.

Vigencia

La vigencia de estas políticas inicia a partir del 12 de Diciembre del 2022. La actualización No. 01 aquí contenida entra en vigencia a partir del

Actualización No.03 del 04-04-2024



Representante Legal.

CONTROL HISTORIAL DE CAMBIOS

Versión	Fecha	Descripción de la modificación
1	1-01-2018	Creación: Se crea la Política de Seguridad de la Información de acuerdo a lineamiento de la Ley 1581 del 2012. Entra en vigencia a partir del 31-07-2020
2	12-12-2022	Se realizó modificación al documento
3	4-04-2024	Revisión y ajuste de la política, donde se agregaron objetivo y control de seguridad de la información y ciberseguridad.