

# POLÍTICA DE PROTECCION DE DATOS

## Introducción

En Quantum Colombia S.A.S., estamos comprometidos con la protección de los datos personales de nuestros clientes, empleados, proveedores y todas las partes interesadas. Esta política establece las directrices y procedimientos que seguimos para garantizar la protección y tratamiento adecuado de los datos personales, conforme a las normativas legales:

- Decreto Único 1074 de 2015
- Decreto 090 del 18 de enero de 2018
- Ley 1581 de 2012
- Ley 1266 de 2008 en Colombia.

Esta política se integra y complementa con los documentos del Sistema de Gestión de Seguridad de la Información (SGSI) de Quantum, entre los que se incluyen:

- **Política General de Seguridad de la Información**
- **Manual de SGSI - Políticas de Seguridad de la Información**
- **Matriz de Control de Acceso**
- **Procedimiento de Gestión de Incidentes de Seguridad de la Información**
- **Programa de Capacitación de SGSI**
- **BCP Quantum**
- **Formato de Registro de Incidentes de Seguridad**

La responsabilidad del tratamiento de datos personales recae en el Oficial de Protección de Datos, cuya posición y responsabilidades están alineadas con la estructura organizacional descrita en la "**Roles y responsables de la gestión de la seguridad de la información, ciberseguridad y los riesgos operacionales**". Este oficial es responsable de supervisar el cumplimiento de la política, la capacitación del personal y la gestión de incidentes relacionados con datos personales.

## Definiciones

- **Dato Personal:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.

- **Dato Público:** Información clasificada como tal por la ley o la Constitución Política, que no es semiprivada, privada o sensible. Incluye datos como el estado civil, profesión u oficio y calidad de comerciante o servidor público.
- **Dato Privado:** Información íntima o reservada que solo es relevante para el titular.
- **Dato Sensible:** Información que afecta la intimidad del titular o cuyo uso indebido puede generar discriminación.
- **Tratamiento:** Cualquier operación o conjunto de operaciones sobre datos personales, tales como recolección, almacenamiento, uso, circulación o supresión.
- **Titular:** Persona natural cuyos datos personales son objeto de tratamiento.
- **Responsable del Tratamiento:** Persona natural o jurídica que decide sobre la base de datos y/o el tratamiento de los datos.
- **Encargado del Tratamiento:** Persona natural o jurídica que realiza el tratamiento de datos personales por cuenta del responsable del tratamiento.

## Principios para el Tratamiento de Datos Personales

Quantum Colombia S.A.S. se compromete a seguir los siguientes principios en el tratamiento de datos personales:

- **Legalidad:** De acuerdo con el Artículo 4 de la Ley 1581 de 2012, el tratamiento de datos personales debe sujetarse a lo establecido en la ley y demás disposiciones normativas aplicables.
- **Finalidad:** Los datos personales serán recolectados y tratados con una finalidad específica, explícita y legítima, informada al titular conforme a lo dispuesto en el Artículo 8 de la Ley 1581 de 2012. Los datos personales recolectados deberán ser utilizados únicamente para los fines informados al titular y autorizados por este.
- **Libertad:** La recolección de datos personales solo se realizará con el consentimiento previo, expreso e informado del titular.
- **Transparencia:** Se garantizará el derecho del titular a obtener información sobre los datos que le conciernen.
- **Seguridad:** Los datos personales serán manejados con medidas de seguridad adecuadas para proteger la información contra accesos no autorizados, alteración o pérdida.

- **Confidencialidad:** Todas las personas que intervengan en el tratamiento de datos personales están obligadas a garantizar la confidencialidad de la información.

## Finalidades del Tratamiento

Los datos personales recolectados por Quantum Colombia S.A.S. serán utilizados para las siguientes finalidades:

- Gestión administrativa y operativa de la empresa.
- Contacto y comunicaciones con clientes, proveedores y empleados.
- Gestión de contratos y cumplimiento de obligaciones contractuales.
- Gestión de recursos humanos, incluyendo contratación, evaluación y capacitación.
- Implementación de medidas de seguridad de la información.
- Cumplimiento de obligaciones legales y regulatorias.
- Reporte a autoridades de control y vigilancia, en caso de ser requerido.
- Realización de estudios internos sobre hábitos de consumo.
- Invitación a eventos organizados por la empresa y envío de información comercial.

## Declaración de Roles y Responsabilidades

Quantum Colombia S.A.S. ha definido claramente los roles y responsabilidades relacionados con la protección de datos personales para asegurar una gestión efectiva:

- **Oficial de Protección de Datos:** Responsable de supervisar la implementación de esta política, liderar el equipo de protección de datos y actuar como punto de contacto principal para las autoridades de control.
- **Jefe de Seguridad de la Información y Ciberseguridad:** Responsable de asegurar que las políticas y procedimientos de protección de datos personales cumplan con las regulaciones y estándares aplicables, incluyendo la ISO 27001.
- **Soporte Técnico de Seguridad:** Responsable de implementar y mantener las herramientas de seguridad necesarias para proteger los datos personales, así como de realizar auditorías periódicas para garantizar la conformidad.

## Programa de Protección de Datos Personales

Se estableció un programa integral de protección de datos personales que se documenta y se revisa periódicamente para asegurar el cumplimiento con la normativa vigente. Este programa incluye:

- **Capacitaciones Anuales:** Obligatorias para todos los empleados, enfocadas en el manejo seguro de datos personales tal y como se menciona en el “**Programa de Capacitación del Sistema de Gestión de Seguridad de la Información**” de Quantum.
- **Evaluaciones Periódicas:** Para medir el nivel de conocimiento del personal sobre las políticas de protección de datos y asegurar su correcta aplicación.
- **Sensibilización Continua:** A través de campañas de concienciación y comunicaciones internas regulares sobre las mejores prácticas en protección de datos.

## Procesos de Evaluación de Impacto a la Privacidad (PIA)

Se ha implementado un Proceso de Evaluación de Impacto a la Privacidad (PIA) para evaluar cualquier nuevo proyecto o cambio que implique el tratamiento de datos personales. Este proceso incluye la evaluación de posibles impactos en la privacidad, la identificación de medidas de mitigación y la aprobación por parte del Oficial de Protección de Datos antes de la implementación.

## Herramientas de Gestión de Riesgos Asociados a Protección de Datos Personales

Se ha implementado una Matriz de Riesgos que permite identificar, evaluar y mitigar los riesgos asociados al tratamiento de datos personales. Esta matriz se actualiza periódicamente para reflejar nuevas amenazas y vulnerabilidades identificadas, y se aplican controles específicos para minimizar estos riesgos.

## Gobierno de protección de datos

Se estableció un gobierno transversal de protección de datos de tres líneas de defensa de forma piramidal siendo la primera línea la base de la pirámide con la particularidad de ejecutar las decisiones tomadas por los niveles superiores, y asumir responsabilidades en menor medida y con mayor generalidad que el resto de las líneas de la pirámide. De tal modo que la tercera línea de defensa tiene la mayor responsabilidad en la toma de decisiones.

Detalle de las líneas de defensa:

1LoD: Es la base de la pirámide compuesta por todos los miembros de la organización los cuales deben cumplir con los siguientes factores:

- Conocimiento: Todos los empleados deben tener un conocimiento básico de las políticas y procedimientos de protección de datos.
- Capacitación continua: Se ofrecen programas de capacitación adaptados a los diferentes roles y niveles de la organización.
- Cultura de seguridad: Se fomenta una cultura donde la protección de datos es una prioridad para todos.
- Cumplimiento de Procedimientos operativos estándar (POE): Cumplen con los pasos a seguir establecidos para cada actividad relacionada con el tratamiento de datos.

2LoD: Es un componente de la organización responsable del seguimiento y evaluación del cumplimiento de la política de protección de datos, adicionalmente se encarga de comunicar a la alta dirección el estado de la organización respecto al cumplimiento normativo mediante KPI y KRI. Adicionalmente detallan los pasos a seguir para cada actividad relacionada con el tratamiento de datos. Finalmente cumplen con la realización de auditorías internas para obtener información objetiva del cumplimiento normativo y procedimental de la protección de datos.

3LoD: Es la cúspide de la pirámide compuesta por la alta dirección que cumple con las siguientes responsabilidades y actividades:

- Comité de protección de datos: Órgano de gobierno encargado de tomar decisiones estratégicas.
- Liderazgo: Proporciona el liderazgo y los recursos necesarios para implementar el modelo.

## Derechos de los Titulares

Los titulares de los datos personales tienen los derechos consagrados en el Artículo 8 de la Ley 1581 de 2012, tales como:

- **Acceso:** Conocer, actualizar y rectificar sus datos personales frente a los responsables y encargados del tratamiento.
- **Revocación y Supresión:** Solicitar la revocación de la autorización y/o la supresión del dato cuando no se respeten los principios, derechos y garantías constitucionales y legales.
- **Prueba de Autorización:** Solicitar prueba de la autorización otorgada para el tratamiento de sus datos personales.
- **Información:** Ser informado sobre el uso dado a sus datos personales.
- **Quejas y Reclamos:** Presentar quejas ante la Superintendencia de Industria y Comercio por infracciones a la normativa vigente.
- **Acceso:** Acceder de manera gratuita a sus datos personales objeto de tratamiento.

## Procedimiento para el Ejercicio de los Derechos

Los titulares de datos personales pueden ejercer sus derechos relacionados con el acceso, actualización, rectificación, supresión y revocación de la autorización para el tratamiento de sus datos personales. Quantum Colombia S.A.S. ha establecido el siguiente procedimiento para garantizar que estas solicitudes sean atendidas de manera oportuna y conforme a la normativa vigente:

### 1. Solicitud Escrita:

El titular debe enviar una solicitud escrita dirigida a Quantum Colombia S.A.S. a través del correo electrónico: [soporte@quantum-la.com](mailto:soporte@quantum-la.com). También se aceptan solicitudes enviadas por correo físico a la dirección de la empresa, la cual deberá estar claramente indicada en la política de privacidad y en todos los formularios relacionados con la protección de datos.

### 2. Contenido de la Solicitud:

La solicitud debe contener la siguiente información:

- **Identificación del Titular:** Nombre completo, número de identificación, y cualquier otro dato que permita la identificación clara del titular.
- **Descripción Clara de la Solicitud:** Una descripción detallada del derecho que desea ejercer, ya sea acceso, actualización, rectificación, supresión o revocación. En el caso de solicitar la rectificación o actualización, se deben adjuntar los documentos que soporten la solicitud.
- **Dirección de Contacto:** Dirección de correo electrónico o física donde se recibirán las notificaciones relacionadas con la solicitud.
- **Documentación Soporte:** Copia de la cédula de ciudadanía o documento de identidad, y en caso de que la solicitud sea realizada por un representante, poder o autorización debidamente otorgada.

### 3. **Recepción y Registro:**

Una vez recibida la solicitud, Quantum Colombia S.A.S. registrará la fecha y hora de recepción, y se asignará un número de referencia único para su seguimiento. Este número será comunicado al titular junto con la confirmación de la recepción de la solicitud.

### 4. **Verificación de Identidad:**

Quantum Colombia S.A.S. se reserva el derecho de verificar la identidad del titular o del representante legal antes de proceder con el trámite de la solicitud. Esta verificación puede incluir la solicitud de documentos adicionales o la validación a través de medios electrónicos.

### 5. **Respuesta:**

Quantum Colombia S.A.S. responderá a la solicitud dentro de los plazos establecidos por la ley, que son:

- **Consultas:** Dentro de los diez (10) días hábiles contados a partir de la fecha de recibo de la solicitud. Si no es posible responder dentro de este plazo, se informará al solicitante sobre las razones de la demora y la fecha en que se dará respuesta, la cual no podrá exceder los cinco (5) días hábiles siguientes al vencimiento del primer término.
- **Reclamos:** Dentro de los quince (15) días hábiles contados a partir de la fecha de recibo del reclamo. Si no es posible responder en este plazo, se informará al titular sobre las razones de la demora y la fecha en que se dará respuesta, la cual no

podrá exceder los ocho (8) días hábiles siguientes al vencimiento del primer término.

**6. Trámite Interno:**

El Oficial de Protección de Datos de Quantum Colombia S.A.S. será responsable de gestionar la solicitud internamente, coordinando con las áreas correspondientes para asegurar que se tome la acción necesaria en relación con la solicitud del titular.

**7. Notificación de Respuesta:**

Una vez procesada la solicitud, Quantum Colombia S.A.S. notificará al titular sobre las acciones tomadas. En caso de que la solicitud implique la corrección, actualización o eliminación de datos, se le informará al titular sobre los cambios realizados.

**8. Archivo y Custodia:**

Todas las solicitudes, junto con las respuestas proporcionadas y los documentos asociados, serán archivadas de manera segura por Quantum Colombia S.A.S., garantizando su conservación conforme a las normas de retención documental aplicables.

**9. Escalamiento de Disputas:**

Si el titular considera que la respuesta a su solicitud no es satisfactoria o si la solicitud no es atendida en los plazos legales, tiene derecho a elevar su queja ante la Superintendencia de Industria y Comercio, en cumplimiento del artículo 16 de la Ley 1581 de 2012.

## **Gestión de Incidentes de Seguridad en el Tratamiento de Datos Personales**

Quantum Colombia S.A.S. reconoce la importancia de gestionar de manera adecuada y eficiente cualquier incidente de seguridad que pueda comprometer la confidencialidad, integridad o disponibilidad de los datos personales. A continuación, se detallan los pasos y procedimientos que se deben seguir en caso de que ocurra un incidente de seguridad relacionado con el tratamiento de datos personales.

### **1. Detección y Notificación Interna**

Todo el personal de Quantum Colombia S.A.S. debe estar capacitado para identificar y reportar de inmediato cualquier incidente de seguridad que comprometa los datos personales. Una vez detectado un incidente, este debe ser reportado inmediatamente al Oficial de Protección de Datos y al equipo de respuesta a incidentes.

## **2. Contención del Incidente**

El equipo de respuesta a incidentes debe tomar medidas inmediatas para contener el incidente y evitar una mayor exposición o pérdida de los datos personales comprometidos. Las acciones pueden incluir la desconexión de sistemas, el aislamiento de redes, o la suspensión de procesos que involucren los datos afectados.

## **3. Evaluación Preliminar**

Se debe realizar una evaluación preliminar para determinar la naturaleza, el alcance y el posible impacto del incidente. Las preguntas clave a responder incluyen: ¿Cómo ocurrió el incidente? ¿Qué tipo de datos fueron comprometidos? ¿Cuál es el impacto potencial sobre los titulares de los datos?

## **4. Evaluación de Riesgos**

Evaluar los riesgos asociados con el incidente es esencial. Se debe considerar la sensibilidad de los datos comprometidos, el número de titulares involucrados y las posibles consecuencias para estos. Dependiendo del riesgo, se determinarán las acciones correctivas a seguir.

## **5. Notificación a la Superintendencia de Industria y Comercio (SIC)**

En caso de un incidente significativo, Quantum Colombia S.A.S. debe notificar a la Superintendencia de Industria y Comercio dentro de los 15 días hábiles siguientes a la detección del incidente, conforme a la Ley 1581 de 2012.

## **6. Comunicación a los Titulares de los Datos**

Si es necesario, se informará a los titulares de los datos personales comprometidos sobre el incidente y las medidas que pueden tomar para protegerse, como cambiar contraseñas, monitorear sus cuentas, etc. La comunicación debe ser clara, precisa y enviada en un plazo oportuno.

## **7. Implementación de Medidas Correctivas**

Se deben adoptar medidas correctivas para evitar la repetición del incidente. Estas pueden incluir mejoras en los controles de seguridad, revisiones de políticas de seguridad y capacitación adicional del personal.

## **8. Documentación y Registro del Incidente**

Todos los detalles del incidente, las acciones tomadas y los resultados de la evaluación de riesgos deben ser documentados y archivados. Este registro será esencial para auditorías y futuras revisiones de las políticas de seguridad.

## **9. Prevención de Futuros Incidentes**

Una vez que se hayan implementado las medidas correctivas, es crucial ejecutar un plan de prevención para evitar futuros incidentes. Esto incluye revisiones periódicas de las políticas de seguridad y la realización de simulacros para evaluar la preparación del equipo.

# **Seguridad de la Información**

Quantum Colombia S.A.S. implementa medidas técnicas, humanas y administrativas necesarias para garantizar la seguridad de los datos personales y evitar su adulteración, pérdida, consulta, uso o acceso no autorizado.

Las medidas de seguridad aplicables al tratamiento de datos personales se detallan en la "Política General de Seguridad de la Información" y el "Manual de SGSI - Políticas de Seguridad de la Información". Estas medidas incluyen controles técnicos, organizacionales y físicos para proteger los datos contra accesos no autorizados, alteración, pérdida o destrucción.

Todo el personal que maneja datos personales será capacitado de acuerdo con el "Programa de Capacitación de SGSI". Esta capacitación se actualizará periódicamente para reflejar las mejores prácticas y cualquier cambio en la normativa aplicable.

# **Identificación de Riesgos Asociados al Tratamiento de Datos Personales**

Quantum Colombia S.A.S. realiza evaluaciones periódicas de riesgos para identificar amenazas y vulnerabilidades en el tratamiento de datos personales. Estos riesgos se gestionan implementando controles específicos, que se documentan y monitorean regularmente.

# Manejo de Incidentes Relacionados con Datos

## Personales

Cualquier incidente relacionado con la seguridad de los datos personales será gestionado conforme al "**Procedimiento de Gestión de Incidentes de Seguridad de la Información**". Esto incluye la notificación de incidentes, la investigación y la implementación de medidas correctivas para mitigar cualquier riesgo derivado.

## Clasificación de la Información

Los datos personales se clasifican según su nivel de sensibilidad en públicos, privados y sensibles. Esta clasificación, alineada con la "**Política General de Seguridad de la Información**" y el documento "**manual de SGSI -políticas de seguridad de la información**", determina los controles aplicables para asegurar su protección adecuada.

## Gestión de Terceros

Cuando los datos personales son compartidos con terceros, Quantum Colombia S.A.S. garantiza que estos cumplan con los mismos estándares de protección. Se establecen contratos y acuerdos de confidencialidad, asegurando que el tratamiento de los datos se realice de acuerdo con esta política y las normativas legales vigentes.

## Transferencia de datos

La transferencia de datos personales solo se realizará en casos específicos y bajo estrictas condiciones de seguridad. Cada vez que se lleve a cabo una transferencia de datos personales, deberá registrarse la siguiente información:

- **Destinatario de la Transferencia:** Identificación de la persona, entidad o área a la que se transfiere la información.
- **Propósito de la Transferencia:** Descripción clara y específica del motivo por el cual se realiza la transferencia de datos.
- **Fechas de la Transferencia:** Registro de las fechas exactas en las que se realiza la transferencia, incluyendo tanto la fecha de inicio como de finalización, si aplica.

- **Responsable de la Transferencia:** Identificación del responsable de supervisar y autorizar la transferencia, asegurando que se realice conforme a las políticas y normativas establecidas.

Este registro será mantenido de manera segura y accesible únicamente para aquellos roles dentro de la organización que tengan la autorización correspondiente, garantizando así la trazabilidad y el cumplimiento de los principios de seguridad de la información.

## Control y Monitoreo de Acceso a Datos Personales

El acceso a los datos personales es monitoreado y auditado regularmente. Los registros de acceso se revisan para detectar actividades inusuales, y se toman medidas correctivas en caso de cualquier incumplimiento.

## Gestión de la Continuidad del Negocio en Relación con Datos Personales

La continuidad del tratamiento de datos personales durante incidentes está asegurada a través del "**BCP Quantum**". Esto garantiza que los datos permanezcan protegidos y que las operaciones críticas continúen durante y después de un incidente, siguiendo las estrategias establecidas para la recuperación ante desastres.

## Procedimientos para la Eliminación de Datos Personales

Cuando los datos personales ya no sean necesarios para las finalidades declaradas, serán eliminados de manera segura, conforme a los procedimientos descritos en la "**Política General de Seguridad de la Información**" y el "**Manual de SGSI - Políticas de Seguridad de la Información**".

## Responsabilidad Legal y Cumplimiento

Quantum Colombia S.A.S. se compromete a cumplir con toda la legislación local e internacional aplicable al tratamiento de datos personales, siguiendo las directrices establecidas en la ISO 27701 para la gestión de la privacidad de la información.

## Modificaciones a la Política

Quantum Colombia S.A.S. se reserva el derecho de modificar esta política en cualquier momento. Cualquier cambio será comunicado a través de los canales habituales y estará disponible en nuestro sitio web [[www.quantumcolombia.com](http://www.quantumcolombia.com)].

Esta política será revisada y actualizada de acuerdo con el "**Procedimiento General de Gestión del Cambio**". Las revisiones se realizarán al menos una vez al año o cuando haya cambios significativos en la legislación o en las prácticas de la empresa.

## Contacto

Para cualquier consulta relacionada con esta política o el tratamiento de sus datos personales, puede contactarnos a través del correo electrónico [seguridad@quantum-la.com](mailto:seguridad@quantum-la.com).