Historial de Cambios o Modificaciones					
Versión	Pág.	Descripción de la Modificación	Realizado Por	Solicitado por	Fecha Ejecución
01	Todo	Elaboración	JC. Ponce	MB. Moreno	09-2024

POLÍTICA

Protección de Datos Personales

PO 2102

DOCUMENTO CONTROLADO

Responsabilidad	Función	Nombre	Firma
Elaborador:	Abogado Senior	Juan Carlos Ponce	
Responsable:	Gerente Legal	Ma. Belén Moreno	
Aprobador:	Gerente General	Francisco Arévalo	

CONTENIDO

1. OBJETIVO 3
2. ALCANCE 3
3. RESPONSABLE Y AUTORIDAD 3
4. DEFINICIONES Y ABREVIACIONES 4
5. DOCUMENTOS RELACIONADOS 6
6. DETALLE DE LA POLÍTICA 6
7. REGISTROS 14
8. LISTA DE DISTRIBUCIÓN 14

DOCUMENTO CONTROLADO

1. OBJETIVO

Establecer una política interna con el objetivo de dar cumplimiento a la normativa relacionada a protección de datos personales, su uso y almacenamiento.

2. ALCANCE

Esta política es aplicable a todos los titulares de datos personales cuyo consentimiento debe otorgarse previamente, así como documentos físicos o digitales que sean objeto de tratamiento por parte de PCR ECUADOR S.A. (en adelante PCR), en su calidad de responsable del Tratamiento de Datos Personales.

3. RESPONSABLE Y AUTORIDAD

FUNCIÓN	RESPONSABILIDAD	AUTORIDAD
Gerente General	Cumplir y hacer cumplir esta política.	Aprobar política
Gerente Legal	Responsable de revisar, cotejar que esta política se alinee con la normativa vigente. Cumplir y hacer cumplir esta política.	Revisar y aprobar los procedimientos e instructivos operativos dentro de su alcance de control
Gerentes de todas las Áreas	Responsable de cumplir y hacer cumplir esta política y realizar seguimiento de cualquier tratamiento de datos personales que se realice en su área a cargo	
Comisión de Protección de Datos Personales	Órgano interno tripartito compuesto por el Gerente General, Gerente de Capital Humano y Gerente Legal, responsable de definir las medidas apropiadas para la observancia efectiva de los principios de protección de datos, así como de los derechos reconocidos en la Ley.	Cumplir con las funciones encomendadas en este procedimiento.
Responsable del Tratamiento de Datos Personales	Es PCR como tal. Responsable de aplicar medidas apropiadas que sean adecuadas para la observancia efectiva de los principios de protección de datos, así como de los derechos reconocidos en la Ley. De igual manera, es quien decide como tratar los datos personales de sus colaboradores.	Cumplir con las funciones encomendadas según ley y este procedimiento.
Responsables Internos	PCR como responsable puede designar responsables internos a través de sus colaboradores. Son colaboradores que por sus funciones realizan el tratamiento de datos personales o tienen conocimiento de datos personales. Cabe señalar que no tienen responsabilidad frente a la autoridad de control de tratamiento de datos personales, puesto que sus funciones son netamente de apoyo.	Mantener la confidencialidad en la información que realizan el tratamiento
Encargado del Tratamiento de Datos Personales	Quien recibe y ofrece garantías suficientes para aplicar medidas técnicas, jurídicas, administrativas y organizativas apropiadas para el adecuado tratamiento de los datos personales y la protección de los derechos de los titulares. Sigue instrucciones y a la vez ayuda al Responsable a	Manejar y administrar los datos personales recibidos para el cumplimiento de sus funciones según la ley y este procedimiento.

DOCUMENTO CONTROLADO

	cumplir sus fines. Puede ser cualquier persona natural o jurídica que recepte datos personales de PCR o sus colaboradores.	
Delegado de Datos Personales	Profesional interno o externo a PCR designado por el responsable para que informe sobre el tratamiento sobre sus obligaciones legales en materia de protección de datos, así como para que se encargue de velar o supervisar el cumplimiento normativo al respecto, y de cooperar, en caso de ser necesario con el Superintendente de Protección de Datos.	Ser el punto de contacto con la Superintendencia de Protección de Datos.
Titular	Persona que otorga su consentimiento a PCR para el tratamiento de sus datos personales.	
Ingeniero de Procesos	Responsable de coordinar que toda la documentación de la empresa esté levantada, actualizada y que la interconexión de procesos en todos los departamentos sea consistente.	

4. DEFINICIONES Y ABREVIACIONES

4.1. Consentimiento. - Manifestación de la voluntad libre, específica, informada e inequívoca, por la que el Titular de los datos personales autoriza al responsable del Tratamiento de Datos Personales a tratar los mismos.

4.2. Dato Personal. - Es cualquier información relacionada con una persona natural identificada o identificable. Esto puede incluir, a manera de ejemplo: nombres, apellidos, números de identificación, direcciones físicas o de correo electrónico, números de teléfono, fotografías, datos biométricos (como huellas dactilares o rasgos faciales), registros financieros, información de salud, opiniones políticas, creencias religiosas, u otra información que pueda utilizarse para identificar directa o indirectamente a una persona.

Se considerarán categorías especiales de Datos Personales, los siguientes:

a) Datos sensibles;
b) Datos de niñas, niños y adolescentes;
c) Datos relacionados a orientación sexual, identidad de género;
d) Datos de salud; y,
e) Datos de personas con discapacidad y de sus sustitutos, relativos a la discapacidad.

4.2.1. Datos Relativos a la salud. - Datos Personales relativos a la salud física o mental de una persona, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud y su historial. Se incluyen todos los datos relativos al estado de salud del titular que dan información sobre su estado de salud física o mental pasado, presente o futuro. Así también contiene la información sobre la persona natural recogida con ocasión de su inscripción a efectos de asistencia sanitaria, o con ocasión de la prestación de tal asistencia; todo número, símbolo o dato asignado a una persona natural que la identifique de manera unívoca a efectos sanitarios; la información obtenida de pruebas o exámenes de una parte del cuerpo o de una sustancia corporal, incluida la procedente de datos genéticos y muestras biológicas, y cualquier información relativa, a título de ejemplo, a una enfermedad, una discapacidad, el riesgo de padecer enfermedades, el

DOCUMENTO CONTROLADO

historial médico, el tratamiento clínico o el estado fisiológico o biomédico del titular, independientemente de su fuente.

Como parte de la Historia clínica ocupacional no se puede solicitar información sobre: orientación sexual, identidad de género, antecedentes ginecobstétricos, antecedentes reproductivos masculinos y hábitos tóxicos.

4.2.2. Datos personales crediticios. - Datos que integran el comportamiento económico de la persona.

4.2.3. Datos étnicos. - Se refieren a información relacionada con la identidad étnica o racial de una persona.

4.3. Datos Primarios. - Información que se recopila directamente de una fuente original. Estos datos son la primera instancia de información y no han sido procesados, analizados o interpretados previamente.

4.4. Datos Públicos. - Aquella información que sí puede ser compartida sin restricciones, esto es la información que consta en una tarjeta de presentación, como es el nombre, cargo, correo electrónico institucional, número de teléfono celular otorgado por la organización y lugar de trabajo.

4.5. Datos Secundarios. - Son aquellos que no se recopilan directamente de la fuente original que pueden obtenerse de fuentes ya existentes. También pueden derivarse de procesos, análisis o interpretación previa por una persona o una aplicación tecnológica. Para que se consideren datos secundarios, cuando se reciban o analicen los mismos no se podrá identificar a una persona especifica con los mismos.

4.6. Delegado de Protección de Datos. - Persona natural encargada de informar al responsable o al Encargado del tratamiento sobre sus obligaciones legales en materia de protección de datos, así como de velar o supervisar el cumplimiento normativo al respecto, y de cooperar con la Autoridad de Protección de Datos Personales, sirviendo como punto de contacto entre esta y la entidad responsable del tratamiento de datos.

4.7. Descargo o Disclaimer. - acuerdo de manejo de datos personales a través del cual el titular de datos personales autoriza al Encargado a utilizar sus datos personales para fines específicos.

4.8. Encargado del Tratamiento de Datos Personales. - Es quien solo o juntamente con otros trate datos personales a nombre y por cuenta de un responsable de tratamiento de datos personales. En este caso son todas aquellas personas naturales o jurídicas intermediarias de información como por ejemplo compañías que realizan el registro de proveedores a nombre de PCR, headhunters, auditores, entre otros.

4.9. Información Confidencial. - Información o documentación, en cualquier formato, final o preparatoria, haya sido o no generada por el sujeto obligado, derivada de los derechos de PCR, personalísimos y fundamentales, que requiere expresa autorización de su titular para su divulgación, y, que contiene datos que, al revelarse, pudiesen dañar los siguientes intereses privados:

a) El derecho a la privacidad, incluyendo privacidad relacionada a vida, salud o seguridad, así como el derecho al honor y la propia imagen;

b) Los datos personales cuya difusión requieran el consentimiento de sus titulares deberán ser tratados según lo dispuesto en la normativa citada en el numeral 5 de esta política;

c) Los intereses comerciales y económicos legítimos; y,

d) Las patentes, derechos de autor y secretos comerciales.

DOCUMENTO CONTROLADO

4.10. Ley. – Toda la normativa citada en el numeral 5 de esta política.

4.11. PCR. - Compañías y consorcios de nacionalidad ecuatoriana que forman parte del holding de PCR en el Ecuador.

4.12. Plazo de Conservación. - El plazo máximo de conservación es el necesario para cumplir con la finalidad de su tratamiento. Para el caso de PCR el plazo establecido es de diez (10) años. Para información relacionada a colaboradores y su información histórica, Capital Humano definirá el tiempo de conservación.

4.13. Registro de Datos Personales de PCR. - Archivo de PCR dentro del cual se almacenan Datos Personales de los Titulares. Es un archivo centralizado en el que deberá constar la información clasificada en distintos ámbitos como Información General, Información de Contacto, Información Académica, Información Laboral, Información de Salud, Información de Seguridad, entre otros. Este registro también lo deberán llevar aquellos contratistas y subcontratistas de PCR que cuenten con más de 100 colaboradores, requisito que deberá ser cubierto a través de la presentación del Anexo D suscrito, previo a la firma del respectivo contrato que le fue adjudicado.

4.14. Responsable del Tratamiento de Datos Personales. - es quien controla, decide y se responsabiliza de la política y las directrices que PCR emite con relación a datos personales.

4.15. Tratamiento. - Es el uso de datos de personas naturales de cualquier forma, automatizada, semi automatizada o no automatizada, que implica la recogida, registro, organización, conservación, custodia, adaptación, modificación, eliminación, indexación, extracción, consulta, elaboración, utilización, posesión, aprovechamiento, distribución, cesión, comunicación, destrucción o cualquier otro tipo de uso o almacenamiento de dicha información.

4.16. Volumen del Negocio (referencia aplicable para sanciones): cuantía resultante de la venta de productos y de la prestación de servicios realizados por operadores económicos, durante el último ejercicio que corresponda a sus actividades, previa deducción del Impuesto al Valor Agregado y de otros impuestos directamente relacionados con la operación económica.

5. DOCUMENTOS RELACIONADOS

- Ley Orgánica de Protección de Datos Personales.
- Sentencia Constitucional 59-19-IN/24.
- Reglamento General de la Ley Protección Datos Personales.
- Reglamento para el Tratamiento de Datos Personales dentro de Procesos Judiciales.
- Ley Orgánica de Transparencia y Acceso a la Información Pública.
- Reglamento General de la Ley Orgánica de Transparencia y Acceso a la Información Pública.
- Reglamento Interno de Trabajo.
- Reglamento de Seguridad y Salud en el Trabajo.
- Código de Ética y Conducta Empresarial de PCR.
- Políticas y procedimientos internos en los que haga uso de datos personales como:
    - PO 2801 Acceso a la Información Pública
    - PR 2701-01 Selección de Personal
    - PR 2701-02 Contratación de Personal
    - PR 2102-01 Calificación de Proveedores

6. DETALLE DE POLÍTICA

DOCUMENTO CONTROLADO

La Política de Protección de Datos constituye un marco normativo organizacional que contiene disposiciones sobre el tratamiento y protección de datos personales que es de obligatorio cumplimiento para los colaboradores, proveedores, contratistas, subcontratistas, compañías relacionadas y accionistas de PCR y que a la vez garantiza el derecho a la información.

6.1 Generalidades del Tratamiento de Datos Personales

6.1.1 El responsable de Datos Personales (es decir PCR) deberá obtener el consentimiento del Titular, el cual deberá ser otorgado de manera libre, específica, informada e inequívoca y además, le deberá indicar, entre otros aspectos, los tipos de tratamiento, finalidades, el tiempo de conservación, las medidas de protección a adoptarse, las consecuencias de su entrega.

6.1.2 El consentimiento del Titular deberá reflejar de manera indubitada la aceptación de éste en relación con el tratamiento de sus datos personales a través de una declaración, pronunciamiento para darse de baja o clara acción afirmativa. La revocatoria del consentimiento no afectará la licitud del tratamiento de datos llevado a cabo hasta el momento de la revocatoria.

6.1.3 La información de datos personales primarios, únicamente podrán ser utilizadas por las áreas de PCR que específicamente lo requieran.

6.1.4 La información recibida solo podrá ser utilizada para el cumplimiento del fin requerido y autorizado por el Titular.

6.1.5 Los Encargados de Tratamiento de Datos que reciban información primaria deberán eliminar la que ya no requieran para el desempeño de sus labores, anualmente. Se exceptúa la información que por cumplimiento normativo o protección e historial de PCR deba almacenarse hasta por 10 años desde su recepción.

6.1.6 El área de la organización a cargo de realizar auditorías internas podrá realizar controles para verificar que se está dando cumplimiento con la eliminación de datos personales.

6.1.7 Cada vez que la organización reciba datos personales de terceros para el cumplimiento de sus actividades, comunicará a estos cómo manejará su información, como la almacenará, en dónde y el tiempo por el que se almacenará. Para ello se requerirá del consentimiento libre de vicios del Titular, el cual constará en el Disclaimer que consta como Anexo A.

6.1.8 Para que PCR reciba datos personales de los colaboradores para el cumplimiento de obligaciones laborales, contractuales o de cualquier otra naturaleza de parte de PCR, ha desarrollado esta política. Para ello se requerirá del consentimiento del Titular, el cual constará en el Disclaimer que consta como Anexo B.

6.1.9 Para el tratamiento de datos sensibles de menores de edad, así como para las decisiones basadas en valoraciones automatizadas de estas personas, se requerirá el consentimiento expreso de su representante legal. (Anexo B). Cuando PCR reciba datos personales de candidatos en procesos de selección para la evaluación de su perfil, tales como su formación y competencias, o incluso para realizar exámenes médicos pre ocupacionales, comunicará a estos cómo manejará su información, como la almacenará, en dónde, el tiempo por el que se almacenará y que áreas tendrán acceso. Para ello se requerirá del consentimiento del Titular, el cual constará en el Disclaimer que consta como Anexo C.

6.1.10 El responsable deberá designar un delegado de Protección de Datos Personales, quien será un profesional externo o interno, y que se encargará principalmente de asesorar al responsable; supervisar el cumplimiento de la normativa de protección de datos personales, así como de las políticas internas de tratamiento de datos personales de PCR; y, ser el punto de contacto con la Autoridad de Protección de datos personales.

6.1.11. El responsable deberá crear una Comisión de Protección de Datos Personales.

6.1.12. El delegado deberá presentar un Informe mensual de actividades a la Comisión de Protección de Datos Personales, así como un informe anual al cierre de cada año.

6.2 Requerimiento directo del Titular del dato de carácter personal al responsable del Tratamiento de Datos:

DOCUMENTO CONTROLADO

El Titular podrá en cualquier momento, de forma gratuita, por medios físicos o digitales puestos a su disposición por parte del Responsable del Tratamiento de Datos Personales, presentar requerimientos, peticiones, quejas o reclamaciones directamente al Responsable del Tratamiento de Datos Personales, relacionadas con el ejercicio de sus derechos, la aplicación de principios y el cumplimiento de obligaciones por parte del Responsable del Tratamiento de Datos Personales, que tengan relación con él. Presentado el requerimiento ante el responsable del Tratamiento de Datos Personales este contará con un término de 10 días para contestar afirmativa o negativamente, notificar y ejecutar lo que corresponda.

Los requerimientos, peticiones quejas o reclamaciones serán atendidos a través de un correo electrónico de PCR que será creado para estos fines

6.3 Obligaciones:

6.3.1 Obligaciones de PCR como responsable:

a) Tratar datos personales en estricto apego a los principios y derechos desarrollados en la Ley Orgánica de Protección de Datos Personales, en su reglamento, en directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales, o normativa sobre la materia;
b) Aplicar e implementar requisitos *y* herramientas administrativas, técnicas, físicas, organizativas y jurídicas apropiadas, a fin de garantizar y demostrar que el tratamiento de datos personales se ha realizado conforme a lo previsto en la Ley, en su reglamento, en directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales, o normativa sobre la materia;
c) Aplicar e implementar procesos de verificación, evaluación, valoración periódica de la eficiencia, eficacia y efectividad de los requisitos y herramientas administrativas, técnicas, físicas, organizativas y jurídicas implementadas;
d) Implementar políticas de protección de datos personales afines al tratamiento de datos personales en cada caso en particular;
e) Utilizar metodologías de análisis y gestión de riesgos adaptadas a las particularidades del tratamiento y de las partes involucradas;
f) Realizar evaluaciones de adecuación al nivel de seguridad previas al tratamiento de datos personales.
g) Tomar medidas tecnológicas, físicas, administrativas, organizativas y jurídicas necesarias para prevenir, impedir, reducir, mitigar y controlar los riesgos y las vulneraciones identificadas;
h) Notificar a la Autoridad de Protección de Datos Personales y al titular de los datos acerca de violaciones a las seguridades implementadas para el tratamiento de datos personales conforme a lo establecido en el procedimiento previsto para el efecto;
i) Implementar esta política de protección de datos personales desde el diseño y por defecto;
j) Suscribir acuerdos de confidencialidad y manejo adecuado de datos personales con el Encargado y el personal a cargo del tratamiento de datos personales o que tenga conocimiento de los datos personales;
k) Solicitar la suscripción de Disclaimers según lo especificado en esta política;
l) Asegurar que el Encargado del Tratamiento de Datos Personales posea mecanismos y herramientas suficientes para garantizar el derecho a la protección de datos personales conforme a lo establecido en la ley, en su reglamento, en directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales, normativa sobre la materia y las mejores prácticas a nivel nacional o internacional, cuando aplique;
m) Designar al delegado de Protección de Datos Personales;
n) Generar un Registro de Protección de Datos Personales de PCR, según lo dispuesto en la normativa; y,

DOCUMENTO NO CONTROLADO

o) Permitir y contribuir a la realización de auditorías o inspecciones, por parte de un auditor acreditado por la Autoridad de Protección de Datos Personales.

6.3.2. Obligaciones del Encargado del Tratamiento de Datos:

a) Cumplir con medidas técnicas y organizativas adecuadas para brindar el servicio y que deberán ser equiparables a aquellas a las que está obligado del responsable.
b) Actuar a nombre y por cuenta del responsable y sus instrucciones documentadas y de considerar que una instrucción es ilegal, informará al responsable del tratamiento para que se corrija la instrucción de ser pertinente.
c) Notificar al responsable sobre la vulneración de la seguridad de datos personales.
d) Devolver o eliminar todos los datos personales, según las instrucciones impartidas por el responsable.
e) Permitir al responsable la revisión de los registros y procesos que tengan relación con los tratamientos de datos personales encomendados.
f) Garantizar que las medidas implementadas sean apropiadas para el adecuado tratamiento de datos personales.

6.3.3. Obligaciones del delegado de Tratamiento de Datos:

a) Asesorar al responsable, al personal del responsable y al Encargado del tratamiento de datos personales, sobre la normativa legal, y lineamientos y demás regulaciones emitidas por la Autoridad de Protección de Datos Personales.
b) Supervisar el cumplimiento de las disposiciones contenidas en la normativa de Protección de Datos Personales y demás regulaciones emitidas por la Autoridad de Protección de Datos Personales.
c) Asesorar en el análisis de riesgo, evaluación de impacto y evaluación de medidas de seguridad, y supervisar su aplicación.
d) Cooperar con la Autoridad de Protección de Datos Personales y actuar como punto de contacto con dicha entidad, con relación a las cuestiones referentes al tratamiento de datos personales.
e) Capacitar a colaboradores de PCR sobre la protección de datos personales.
f) Cooperar en investigaciones y auditorías.

6.3.4. Obligaciones de la Comisión de Protección de Datos Personales:

a) Establecer los requisitos *y* herramientas administrativas, técnicas, físicas, organizativas y jurídicas apropiadas;
b) Aprobar los procesos de verificación, evaluación, valoración periódica de la eficiencia, eficacia y efectividad de los requisitos y herramientas administrativas, técnicas, físicas, organizativas y jurídicas implementadas;
c) Aprobar las políticas de protección de datos personales afines al tratamiento de datos personales en cada caso en particular;
d) Aprobar las metodologías de análisis y gestión de riesgos adaptadas a las particularidades del tratamiento y de las partes involucradas.
e) Aprobar evaluaciones de adecuación al nivel de seguridad previas al tratamiento de datos personales.
f) Aprobar las medidas tecnológicas, físicas, administrativas, organizativas y jurídicas necesarias para prevenir, impedir, reducir, mitigar y controlar los riesgos y las vulneraciones identificadas.

6.4 Derechos:

Los Derechos que tienen los Titulares sobre sus datos personales son los siguientes:

a) Derecho a la información.
b) Derecho de acceso.
c) Derecho de rectificación y actualización.

DOCUMENTO CONTROLADO

d) Derecho de eliminación.
e) Derecho de oposición.
f) Derecho de portabilidad.
g) Derecho a la suspensión del tratamiento.
h) Derecho a no ser objeto de una decisión basada únicamente en valoraciones automatizadas.
i) Derecho de consulta.

6.4.1 Derecho a la Información:

El Titular de datos personales tiene derecho a ser informado conforme los principios de lealtad y transparencia por cualquier medio sobre:

a) Los fines del tratamiento;
b) La base legal para el tratamiento;
c) Tipos de tratamiento;
d) Tiempo de conservación;
e) La existencia de una base de datos en la que constan sus datos personales;
f) El origen de los datos personales cuando no se hayan obtenido directamente del titular;
g) Otras finalidades y tratamientos ulteriores;
h) Identidad y datos de contacto del responsable del tratamiento de datos personales, que incluirá: dirección del domicilio legal, número de teléfono y correo electrónico;
i) Cuando sea del caso, identidad y datos de contacto del delegado de protección de datos personales, que incluirá: dirección laboral, número de teléfono y correo electrónico;
j) Las transferencias o comunicaciones, nacionales o internacionales, de datos personales que pretenda realizar, incluyendo los destinatarios y sus clases, así como las finalidades que motivan la realización de estas y las garantías de protección establecidas;
k) Las consecuencias para el titular de los datos personales de su entrega o negativa a ello;
l) El efecto de suministrar datos personales erróneos o inexactos;
m) La posibilidad de revocar el consentimiento;
n) La existencia y forma en que pueden hacerse efectivos sus derechos de acceso, eliminación, rectificación y actualización, oposición, anulación, limitación del tratamiento y a no ser objeto de una decisión basada únicamente en valoraciones automatizadas.
o) Los mecanismos para hacer efectivo su derecho a la portabilidad, cuando el titular lo solicite;
p) Dónde y cómo realizar sus reclamos ante el responsable del tratamiento de datos y la Autoridad de Protección de Datos Personales, y;
q) La existencia de valoraciones y decisiones automatizadas, incluida la elaboración de perfiles.

6.4.2 Derecho al Acceso:

El Titular tiene derecho a conocer y a obtener, gratuitamente, del responsable del Tratamiento de Datos Personales acceso a todos sus datos personales, sin necesidad de presentar justificación alguna. El responsable del Tratamiento de Datos Personales deberá establecer métodos razonables que permitan el ejercicio de este derecho, el cual deberá ser atendido en el término de 10 días.
El derecho de acceso no podrá ejercerse de forma tal que constituya abuso del derecho.

6.4.3 Derecho de rectificación y actualización:

El Titular tiene el derecho a obtener del responsable del Tratamiento la rectificación y actualización de sus datos personales inexactos o incompletos.

Para tal efecto, el Titular deberá presentar los justificativos del caso, cuando sea pertinente. El responsable de Tratamiento deberá atender el requerimiento en un término de 15 días y en este mismo termino, deberá informar al destinatario de los datos, de ser el caso, sobre la rectificación, a fin de que lo actualice.

6.4.4 Derecho de eliminación:

DOCUMENTO

El Titular tiene derecho a que el responsable del Tratamiento de Datos Personales suprima sus datos personales, cuando:

a) El tratamiento no cumpla con los principios establecidos en la Ley Orgánica de Protección de Datos Personales;
b) El tratamiento no sea necesario o pertinente para el cumplimiento de la finalidad;
c) Los datos personales hayan cumplido con la finalidad para la cual fueron recogidos o tratados;
d) Haya vencido el plazo de conservación de los datos personales;
e) El tratamiento afecte derechos fundamentales o libertades individuales;
f) Revoque el consentimiento prestado o señale no haberlo otorgado para uno o varios fines específicos, sin necesidad de que medie justificación alguna; o,
g) Exista obligación legal.

El responsable del Tratamiento de Datos Personales implementará métodos y técnicas orientadas a eliminar, hacer ilegible, o dejar irreconocibles de forma definitiva y segura los datos personales. Esta obligación la deberá cumplir en el término de 15 días de recibida la solicitud por parte del Titular y será gratuito.

6.4.5 Derecho de Oposición:

El Titular tiene el derecho a oponerse o negarse al tratamiento de sus datos personales, en los siguientes casos:

a) No se afecten derechos y libertades fundamentales de terceros, la ley se lo permita y no se trate de información pública, de interés público o cuyo tratamiento está ordenado por la ley.
b) Cuando no sea necesario su consentimiento para el tratamiento como consecuencia de la concurrencia de un interés legítimo, y se justifique en una situación concreta personal del Titular, siempre que una ley no disponga lo contrario.

El responsable de Tratamiento de Datos Personales dejará de tratar los datos personales en estos casos, salvo que acredite motivos legítimos e imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del titular, o para la formulación, el ejercicio o la defensa de reclamaciones.
Esta solicitud deberá ser atendida en el término de 10 días.

6.4.6 Derecho a la portabilidad:

El Titular tiene el derecho a recibir del responsable del Tratamiento de Datos Personales, sus datos personales en un formato compatible, actualizado, estructurado, común, interoperable y de lectura mecánica, preservando sus características; o a transmitirlos a otros responsables.

6.4.7 Derecho a la suspensión del tratamiento:

El Titular tendrá derecho a obtener del responsable del Tratamiento de Datos Personales la suspensión del tratamiento de los datos cuando se cumpla alguna de las condiciones siguientes:

a) Cuando el Titular impugne la exactitud de los datos personales, mientras el responsable de Tratamiento verifica la exactitud de estos;
b) El tratamiento sea ilícito y el interesado se oponga a la supresión de los datos personales y solicite en su lugar la limitación de su uso;
c) El responsable ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones; y.
d) Cuando el interesado se haya opuesto al tratamiento; mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado.

6.4.8 Derecho a no ser sujeto de una decisión basada únicamente en valoraciones automatizadas:

DOCUMENTO CONTROLADO

Además de los presupuestos establecidos en el derecho a no ser objeto de una decisión basada única o parcialmente en valoraciones automatizadas, el tratamiento de datos sensibles o datos de niñas, niños y adolescentes deberá contar con el Disclaimer firmado por su representante legal. Los adolescentes, en ejercicio progresivo de sus derechos, a partir de los 15 años, podrán otorgar, en calidad de Titulares, su consentimiento explícito para el tratamiento de sus datos personales, siempre que se les especifique con claridad sus fines.

6.4.9 Derecho de consulta:

Las personas tienen derecho a la consulta de sus Datos Personales ante el Registro de Protección de Datos Personales de PCR.

6.5 Medidas:

Para la materialización de esta Política se debe además contar con lo siguiente:

a) Acuerdos o Disclaimers de Confidencialidad con los colaboradores:

PCR en su calidad de responsable debe solicitar a las personas suscribir los disclaimers y almacenar los mismos. Los correspondientes a los colaboradores y aplicantes a plazas de trabajo los almacenará Capital Humano. Los disclaimers de proveedores y subcontratistas, firmarán parte del expediente del contrato o compra y se subirán al repositorio de contratos de PCR.

b) Aplicación de medidas técnicas:

PCR debe establecer las medidas técnicas para el tratamiento y riesgos que aún no las tenga. A continuación, se describen algunos ejemplos de medidas:

- Cifrado de datos.
- Mecanismos de control de accesos.
- Segmentación de la red.
- Herramientas de control físico.
- Copias de seguridad.
- Firewall.
- Restauración de Sistemas.

c) Aplicación de medidas organizativas:

Además de la Política de Protección de Datos Personales, PCR puede implementar otras medidas organizativas, como, por ejemplo:

- Capacitación a colaboradores.
- Política de control documental (conservación y eliminación).
- Política de Gestión y Seguridad de la Información.
- Política de Acceso a la Información Pública.

d) Aplicación de medidas jurídicas:

Además de los Acuerdos y Disclaimer, PCR debe establecer medidas jurídicas cómo:

- Adaptación de los contratos a esta política y la normativa vigente.
- Suscripción de Acuerdos con los Encargados de Tratamiento de Datos Personales.
- Suscripción de un acuerdo con el delegado de Protección de Datos Personales.

e) Aplicación de medidas se supervisión y control:

PCR debe implementar las siguientes medidas de supervisión y control:

- Auditorías periódicas.
- Monitoreo continuo.
- Planes de contingencia y recuperación.

6.6. Vulneraciones a la Seguridad de Datos Personales y Evaluación de Impacto:

DOCUMENTO CONTROLADO

La vulneración o violación a la seguridad de los datos personales constituye un riesgo para los derechos y las libertades de los titulares cuando:
i) los datos fueron destruidos, ya no existen o no están disponibles de una forma que sea de utilidad para el responsable;
ii) cuando los datos personales hayan sido alterados, corrompidos o dejan de estar completos;
iii) cuando el responsable del tratamiento ha perdido el control o el acceso a los datos o ya no están en su poder; y,
iv) cuando el tratamiento no ha sido autorizado o es ilícito, lo cual incluye la divulgación de datos personales o el acceso por parte de destinatarios que no están autorizados a recibir o acceder a los datos o cualquier otra forma de tratamiento que se ejecuta en contrario a las disposiciones legales.

6.6.1. Notificación de vulneración de seguridad:
El responsable del Tratamiento de Datos Personales a través del delegado de Protección de Datos Personales deberá notificar la vulneración de la seguridad de datos personales a la Autoridad de Protección de Datos Personales, tan pronto sea posible, y a más tardar en el término de 5 días después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si la notificación a la Autoridad de Protección de Datos no tiene lugar en el término de 5 días, deberá ir acompañada de indicación de los motivos de la dilación.

El Encargado del Tratamiento deberá notificar al responsable cualquier vulneración de la seguridad de datos personales tan pronto sea posible, y a más tardar dentro del término de 2 días contados a partir de la fecha en la que tenga conocimiento de ella.

6.7. Evaluación de Impacto:
El responsable realizará una evaluación de impacto del tratamiento de datos personales cuando se haya identificado la probabilidad de que dicho tratamiento, por su naturaleza, contexto o fines, conlleve un alto riesgo para los derechos y libertades del titular o cuando la Autoridad de Protección de Datos Personales lo requiera.
Con respecto a los casos en los cuáles la evaluación de impacto es obligatoria, esta se la deberá presentar ante la Autoridad de Protección de Datos Personales y contendrá, al menos, lo siguiente:
1. La descripción sistemática de las operaciones de tratamiento y las finalidades de ese tratamiento;
2. La justificación de la necesidad de llevar a cabo esas operaciones de tratamiento, así como su proporcionalidad con respecto de la finalidad;
3. La evaluación de riesgos a los derechos y libertades de los titulares; y,
4. Las medidas previstas para hacer frente a los riesgos, las garantías, medidas de seguridad y mecanismos destinados a salvaguardar y demostrar el respeto al derecho de los titulares a la protección de sus datos personales.

6.8. Gestión de Incidentes:
Es necesario generar un procedimiento de Gestión de Incidentes para lo cual se debe incluir dentro de las atribuciones del Comité. En caso de producirse un incidente, el delegado deberá analizar si hay necesidad de notificar el incidente a la Autoridad de Protección de Datos Personales en un plazo máximo de 5 días hábiles desde que tuvo conocimiento.

En la notificación a la Autoridad de Protección de Datos Personales el Gestor explicará las medidas que se han tomado para mitigar la filtración, así como las lecciones aprendidas y que han sido incorporadas a los planes de gestión de incidentes de PCR.

7. REGISTROS

CODIFICACIÓN	DESCRIPCIÓN	RESPONSABLE	TIEMPO DE RETENCIÓN

8. LISTA DE DISTRIBUCIÓN

CONTROL DE DISTRIBUCIÓN				
Ubicación del documento	Usuario	Distribución es		Tipo de Copia
		Controlada	No Controlada	
Empresa	Todos		X	Digital/Papel
Partes Interesadas interna - Quito			X	Digital/Papel
Partes Interesadas interna – Campo			X	Digital/Papel

DOCUMENTO CONTROLADO