POLÍTICA GENERAL DE USO, MANEJO, CONSERVACIÓN Y ELIMINACIÓN DE LA INFORMACIÓN

En cumplimiento de la Ley Orgánica de Protección de Datos Personales del Ecuador (LOPDP) y normativa aplicable, BULLSUPPLY C.A. establece la presente Política General de Uso, Manejo, Conservación y Eliminación de la Información, aplicable a todos los datos personales y corporativos tratados por la empresa, independientemente del medio de recopilación.

1. Alcance

La presente política aplica a:

- Toda información personal o corporativa recopilada a través de:
- WhatsApp y otros servicios de mensajería instantánea.
- Página web institucional y formularios digitales.
- Correo electrónico corporativo.
- Contratos, cotizaciones y documentación física.
- Llamadas telefónicas.
- Redes sociales oficiales.
- Colaboradores, directivos, proveedores y terceros que tengan acceso a información.
- Todo el ciclo de vida del dato: recopilación, uso, almacenamiento, acceso, conservación, transferencia y eliminación.

2. Principios Rectores

El tratamiento de la información se regirá por los siguientes principios:

- Legalidad
- Finalidad

- Proporcionalidad
- Calidad y exactitud
- Seguridad
- Confidencialidad
- Responsabilidad proactiva

3. Finalidades del Tratamiento

La información podrá ser utilizada exclusivamente para:

- Atención de consultas, solicitudes o reclamos.
- Gestión comercial, contractual y administrativa.
- Emisión de cotizaciones, facturación y cumplimiento tributario.
- Cumplimiento de obligaciones legales o regulatorias.
- Gestión de relaciones comerciales y seguimiento de servicios.
- Conservación probatoria en caso de controversias administrativas, judiciales o contractuales.
- Envío de información comercial o promocional, previo consentimiento.
- Queda prohibido el uso de la información para fines distintos a los aquí establecidos.

4. Manejo y Seguridad de la Información

BULLSUPPLY C.A. implementa medidas técnicas y organizativas como:

- Control de accesos restringidos.
- Autenticación en dos pasos.
- Uso de dispositivos corporativos controlados.

- Prohibición de respaldo en dispositivos personales.
- Cifrado de información sensible.
- Protocolos internos de confidencialidad.
- Auditorías periódicas de seguridad.

5. Conservación y Proceso de Eliminación de la Información

5.1 Conservación

La información será conservada únicamente durante:

- El tiempo necesario para cumplir la finalidad del tratamiento.
- El plazo exigido por normativa legal, tributaria o contractual.
- El tiempo necesario para fines probatorios en caso de controversias.

5.2 Proceso General de Eliminación

Una vez cumplida la finalidad o vencido el plazo legal o el plazo interno de 1 año, se activará el siguiente procedimiento:

- Identificación del dato a eliminar.
- Verificación de inexistencia de obligación legal de conservación.
- Autorización interna del responsable del tratamiento.

Eliminación segura mediante:

- Borrado permanente digital.
- Limpieza de respaldos.
- Eliminación de copias en servidores, en cada revisión semestral u anual.
- Destrucción física segura si corresponde.

5.3 Eliminación de Información Recopilada vía WhatsApp

Respecto a información recibida por mensajería instantánea:

- Las conversaciones serán revisadas periódicamente.

- Se eliminarán mensajes y archivos que ya no sean necesarios para fines comerciales o legales.

- Los respaldos serán controlados y depurados conforme sea evaluado.
- Se evitará almacenamiento indefinido en el historial de chats.

5.4 Eliminación de Información Recopilada vía Página Web

En relación con formularios web:

Los datos serán almacenados únicamente en servidores seguros, que cuenta con las debidas medidas de seguridad.

Una vez cumplida la finalidad (cotización, contacto, contratación), los datos serán:

- Eliminados del formulario activo.
- Depurados de bases de datos de contacto si no existe relación contractual u obligación legal.
- Se realizará revisión semestral de bases de datos digitales.
- No se conservarán datos de formularios inactivos o abandonados más allá del tiempo razonable de gestión.

6. Incidentes de Seguridad

En caso de vulneración de seguridad:

- Se activará protocolo interno inmediato.
- Se evaluará el riesgo
- Se notificará a la Autoridad de Protección de Datos cuando corresponda.
- Se informará al titular si existe riesgo significativo.

8. Actualización

La empresa podrá actualizar esta política en función de cambios normativos, tecnológicos o operativos. La versión vigente estará disponible en la página web institucional.