| 1. POLÍTICA DE TRATAMIENTO DE INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES | |
|---|---|
| **RAZON SOCIAL** | **KIOTO SEGURIDAD PRIVADA LTDA.** |
| **NIT** | 9003512196 |
| **Representante Legal** | **YIRLEY ÁLZATE PÉREZ** |
| **Identificación** | 1.152.695.995 |
| **Dirección** | Cl. 49 AA # 77C – 103, Laureles – Medellín. |
| **Teléfono** | 323 585 5935 |
| **Correo electrónico** | gerenciamed@seguridadkioto.com |

## 2. OBJETIVO

La presente Política tiene como finalidad establecer de manera integral los lineamientos, procedimientos, controles y responsabilidades aplicables al tratamiento de datos personales por parte de **KIOTO SEGURIDAD PRIVADA LTDA.**, en desarrollo de su objeto social como empresa prestadora de servicios de vigilancia y seguridad privada.

En particular, esta política busca garantizar el respeto por el derecho fundamental al Habeas Data, asegurando que toda recolección, almacenamiento, uso, circulación, análisis, transmisión, transferencia y supresión de datos personales se realice bajo estándares de legalidad, seguridad, confidencialidad y responsabilidad reforzada, teniendo en cuenta la naturaleza sensible y estratégica de la información manejada en el sector de seguridad privada.

Adicionalmente, se establecen medidas especiales orientadas a:

- La protección de información crítica relacionada con esquemas de seguridad
- La confiabilidad del personal operativo (vigilantes, escoltas, supervisores)
- La trazabilidad de eventos de seguridad
- La prevención de riesgos operacionales, jurídicos y reputacionales

## 3. ALCANCE

Esta Política aplica a todas las bases de datos personales administradas por LA EMPRESA, tanto en medios físicos como digitales, incluyendo aquellas que se encuentren bajo su custodia directa o en administración de terceros encargados.

Cubre el tratamiento de datos personales de:

- Clientes corporativos y residenciales
- Usuarios de servicios de vigilancia fija, móvil o electrónica
- Personal operativo (vigilantes, escoltas, operadores de medios tecnológicos)
- Personal administrativo
- Aspirantes a cargos operativos o administrativos
- Proveedores de tecnología, armas, equipos y logística
- Visitantes a instalaciones protegidas o sedes administrativas
- Personas registradas en sistemas de control de acceso
- Personas captadas por sistemas de videovigilancia

Esta política se aplica a todos los procesos internos de LA EMPRESA, incluyendo:

- Operaciones de seguridad
- Gestión humana
- Gestión administrativa y financiera
- Gestión de riesgos
- Sistemas de información y monitoreo

## 4. MARCO NORMATIVO ESPECIALIZADO

Además de la normativa general de protección de datos, LA EMPRESA da cumplimiento a las disposiciones aplicables al sector de vigilancia, incluyendo:

- Ley 1581 de 2012
- Decreto 1377 de 2013
- Decreto Ley 356 de 1994 (Estatuto de Vigilancia y Seguridad Privada)
- Normativa de la Superintendencia de Vigilancia y Seguridad Privada
- Circulares externas en materia de control, confiabilidad y seguridad

## 5. PRINCIPIOS REFORZADOS PARA EL SECTOR DE VIGILANCIA

Dado el carácter estratégico del servicio de seguridad privada, LA EMPRESA adopta, además de los principios legales, los siguientes principios reforzados:

### 5.1 Principio de Confidencialidad Operacional

La información relacionada con esquemas de seguridad, rutas, protocolos, dispositivos tecnológicos, ubicación de cámaras, turnos y personal asignado tendrá carácter estrictamente reservado.

### 5.2 Principio de Necesidad y Proporcionalidad

Solo se recolectarán los datos estrictamente necesarios para:

- Garantizar la seguridad
- Evaluar la confiabilidad del personal
- Cumplir con obligaciones legales del sector

### 5.3 Principio de Seguridad Reforzada

Los datos personales, especialmente sensibles, serán protegidos mediante medidas técnicas, humanas y administrativas de nivel alto, considerando el impacto que tendría su filtración.

### 5.4 Principio de Reserva Estratégica

La información que, por su naturaleza, pueda comprometer la seguridad, la operación o la integridad del personal, será tratada como información estratégica y de acceso restringido. Su divulgación, uso o reproducción solo podrá realizarse previa autorización expresa de la Alta Dirección o del área competente, bajo estrictos controles de seguridad.

## 6. DERECHO DE LOS TITULARES

- Conocer, actualizar y rectificar sus datos
- Solicitar prueba de autorización
- Revocar autorización
- Solicitar supresión
- Presentar quejas ante la SIC
- Ser informados sobre el uso de sus datos

## 7. PROCEDIMIENTO DE CONSULTAS Y RECLAMOS

- Como titular puede ejercer sus derechos
- Correo electrónico / canal
- Términos de respuesta (10 días hábiles consultas, 15 días hábiles reclamos – Ley 1581)

## 8. AUTORIZACIÓN DEL TITULAR

LA EMPRESA solicitará autorización previa, expresa e informada para el tratamiento de datos personales, indicando claramente:

- Las finalidades específicas del tratamiento
- El carácter facultativo de los datos sensibles
- Los derechos del titular
- Los canales de atención

En el caso del personal operativo, la autorización incluirá de manera expresa:

- Verificación de antecedentes judiciales, disciplinarios y financieros
- Estudios de seguridad
- Uso de información biométrica
- Aplicación de pruebas de confiabilidad (incluyendo polígrafo, cuando aplique)

El titular no está obligado a autorizar el tratamiento de datos sensibles.

## 6. TRATAMIENTO Y FINALIDADES ESPECÍFICAS DEL SECTOR

### 6.1 Clientes (ENFOQUE SECTORIAL)

Además de las finalidades generales, LA EMPRESA tratará datos para:

- Diseñar esquemas de seguridad personalizados
- Elaborar análisis de vulnerabilidad
- Determinar puntos críticos de riesgo
- Coordinar planes de reacción ante incidentes
- Registrar novedades de seguridad
- Documentar eventos, incidentes y reportes operativos

### 6.2 Personal Operativo de Seguridad

Dada la naturaleza del servicio, LA EMPRESA realizará un tratamiento intensivo y especializado de los datos, incluyendo:

- Validación de identidad
- Verificación de antecedentes en bases de datos públicas y privadas
- Estudios de seguridad domiciliarios
- Evaluación de entorno social y económico
- Pruebas de confiabilidad
- Registro de desempeño en servicio
- Seguimiento disciplinario

Asimismo, se podrá tratar información relacionada con:

- Porte y uso de armas
- Certificaciones y permisos
- Historial de turnos y ubicaciones
- Reportes de incidentes

### 6.3 Videovigilancia y Monitoreo Electrónico

LA EMPRESA implementa sistemas de videovigilancia en:

- Instalaciones propias
- Puestos de servicio
- Centros de monitoreo
- Se instalarán avisos visibles informando la existencia de videovigilancia

Las imágenes podrán ser utilizadas para:

- Prevención de delitos
- Identificación de personas
- Control de acceso
- Investigación de incidentes
- Soporte probatorio ante autoridades

Se informa que:

- Las imágenes podrán ser compartidas con autoridades competentes
- Serán almacenadas por el tiempo estrictamente necesario
- Tendrán acceso restringido

## 10. DATOS SENSIBLES (ENFOQUE ESTRICTO)

En el sector de vigilancia, el tratamiento de datos sensibles es necesario, legítimo y proporcional, particularmente en relación con:

- Datos biométricos
- Información de salud ocupacional
- Resultados de pruebas de confiabilidad
- Imágenes de videovigilancia

LA EMPRESA garantiza:

- Tratamiento restringido
- Acceso controlado
- Almacenamiento seguro
- Uso exclusivo para fines autorizados

## 11. SEGURIDAD DE LA INFORMACIÓN (NIVEL EMPRESARIAL)

LA EMPRESA implementa un sistema integral de seguridad de la información que incluye:

### 8.1 Controles Técnicos

- Sistemas de monitoreo
- Cifrado de bases de datos
- Control de accesos por roles
- Registro de accesos (logs)

### 8.2 Controles Operativos

- Protocolos de manejo de información
- Procedimientos de reporte de incidentes
- Auditorías internas

### 8.3 Controles Humanos

- Acuerdos de confidencialidad
- Capacitación continua
- Evaluaciones periódicas de confiabilidad

## 12. GESTIÓN DE INCIDENTES DE SEGURIDAD

En caso de incidentes que comprometan datos personales, LA EMPRESA:

- Activará protocolos internos de respuesta
- Evaluará el impacto del incidente
- Tomará medidas correctivas inmediatas
- Informará a la autoridad competente cuando sea requerido
- Documentará el evento para fines de mejora continua

## 13. TRANSFERENCIA Y TRANSMISIÓN DE DATOS (SECTORIAL)

LA EMPRESA podrá compartir información con:

- Autoridades judiciales y de policía
- Entidades de control
- Clientes (dentro del marco contractual)
- Empresas aliadas de seguridad

Siempre garantizando:

- Confidencialidad
- Seguridad
- Uso limitado a la finalidad autorizada

## 14. PERÍODO DE CONSERVACIÓN

Los datos serán conservados teniendo en cuenta:

- La duración del contrato
- La naturaleza del servicio de seguridad
- Obligaciones legales del sector
- Requerimientos de autoridades

En algunos casos, la información podrá conservarse por períodos prolongados debido a:

- Investigaciones
- Procesos judiciales
- Historial de seguridad

## 15. RESPONSABLE DE PROTECCIÓN DE DATOS

LA EMPRESA designará un área responsable, así como un canal oficial de comunicación (correo electrónico), es decir, un Oficial de Protección de Datos, quien será el encargado de velar por el cumplimiento de las disposiciones legales y políticas internas en materia de tratamiento de datos personales.

- Supervisar el cumplimiento de la política
- Atender consultas y reclamos
- Coordinar auditorías
- Gestionar riesgos en materia de datos