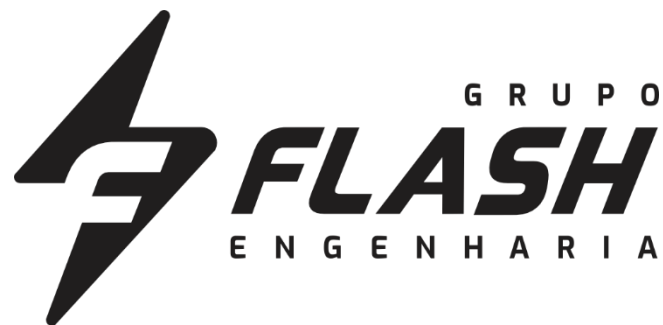


PROGRAMA DE ADECUACIÓN: LEY GENERAL DE PROTECCIÓN DE DATOS PERSONALES



POLÍTICA DE USO DE CÁMARAS (CCTV)

1. INTRODUCCIÓN

La tecnología del Circuito Cerrado de Televisión (CCTV) ha evolucionado en los últimos años para ser más confiable, económica y accesible. Cuando se utiliza adecuadamente, el CCTV puede ayudar a reducir el riesgo de acceso no autorizado a las instalaciones, brindar tranquilidad a los usuarios y proporcionar un registro preciso de lo sucedido en caso de un incidente.

A fin de proteger a sus usuarios, empleados y otras partes interesadas, **FLASH ENGENHARIA** utiliza el CCTV en circunstancias apropiadas para abordar áreas específicas de riesgo. Al recopilar y utilizar estos datos de vídeo grabados, FLASH ENGENHARIA está sujeta a diversas leyes, incluida la Ley 13.709/18 - Ley General de Protección de Datos (LGPD), que regula cómo se deben realizar dichas actividades y las protecciones que deben implementarse para proteger los datos de vídeo registrados.

El objetivo de esta política es definir las reglas que deben seguirse para que las responsabilidades de FLASH ENGENHARIA se cumplan en todo momento y la utilidad de los datos grabados sea conforme a la determinación legal.

2. OBJETIVO

2.1 Los equipos utilizados en el sistema de CCTV son para la seguridad de sus colaboradores, usuarios, proveedores y visitantes en general, bienes e información, con el fin de prevenir hurtos, prácticas de acoso sexual y riesgos relacionados con la seguridad interna. El uso de estos equipos para disuasión podrá dar lugar a la apertura de una investigación y a un potencial proceso penal por comportamiento sospechoso y/o delictivo.

2.2 La empresa **FLASH ENGENHARIA**, inscrita bajo el CNPJ N° 04.844.206/0001-59, con sede en Rua Professora Celia Cangro Marques Mendes, n° 1000 - Alto da Boa Vista - Sorocaba, SP - CEP 18.087-171, opera un sistema de videovigilancia en todas sus instalaciones con la finalidad restringida de promover la seguridad y protección corporativa, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales grabados en formato de imagen, en cumplimiento de la Ley n. 13.709 (LGPD), la ordenanza N° 3.233/2012/DG/DPF, la Constitución de la República Federativa del Brasil (Art. 5°) y la CLT (Leyes del Trabajo), siguiendo también las directrices de la ANPD (Autoridad Nacional de Protección de Datos).

2.3 Esta política no aborda el uso de tecnología especializada, como el Reconocimiento Automático de Matrículas (LPR), reconocimiento facial o vehículos operados remotamente (drones o VANT).

2.4 Esta política se aplica a todas las operaciones, personas y procesos que constituyen los sistemas de seguridad de la información de FLASH ENGENHARIA, incluyendo miembros del consejo, directores, empleados, proveedores y terceros legitimados que puedan tener acceso al sistema de CCTV.

3. PROTECCIÓN DE DATOS

3.1 El sistema de videovigilancia de FLASH ENGENHARIA tiene un propósito específico y legítimo que atiende a una necesidad o área de riesgo, como la prevención o reducción de delitos en lugares sujetos a actividades ilegales.

3.2 Conforme al principio de minimización de datos de la LGPD, la grabación de vídeo debe estar activa solo en los días y horarios necesarios, y la grabación de audio solo se utilizará cuando esté justificada por motivos de privacidad. FLASH ENGENHARIA actuará como el **Controlador de Datos** y, cuando sea necesario, realizará el registro ante la autoridad supervisora.

3.3 Cuando se utilice a un tercero para el tratamiento de imágenes (almacenamiento o

mantenimiento), este será considerado un **Encargado del Tratamiento** (Operador) bajo la LGPD, mediando contrato vigente y adherente al servicio.

3.4 Para cada implementación de un nuevo dispositivo, se realizará una evaluación de impacto de protección de datos (DPIA) para garantizar la protección adecuada de los derechos del titular. La base legal para el tratamiento es la promoción de la seguridad y protección corporativa.

3.5 FLASH ENGENHARIA realizará anualmente una revisión de cumplimiento de la presente política.

4. ESPACIOS CUBIERTOS

4.1 La ubicación de las cámaras busca mantener un perímetro de seguridad y controlar los accesos externos sin vulnerar los derechos de los ciudadanos. La cobertura abarca el espacio físico interno y externo bajo responsabilidad de la empresa, sin enfocarse directamente en el colaborador para no violar su privacidad (Art. 5º inciso X).

4.2 Las cámaras se encuentran en puntos estratégicos: naves de producción, perímetro externo, porterías, entre otros, minimizando la vigilancia en espacios no relevantes para los fines previstos.

5. SEÑALIZACIÓN

5.1 Los lugares con videovigilancia deberán estar obligatoriamente señalizados con avisos o placas, cuyo texto sea compatible con el principio de transparencia de la LGPD.

6. ALMACENAMIENTO Y RETENCIÓN

6.1 El almacenamiento de imágenes será de un mínimo de 7 días y un máximo de 45 días, o según la capacidad del hardware.

6.2 El almacenamiento debe mantenerse en un lugar seguro con acceso restringido a personal autorizado.

6.3 Los "registros de vigilancia" se retendrán por un periodo no superior a **02 (dos) años**, tras los cuales serán borrados o sobrescritos, salvo que formen parte de una investigación criminal o proceso judicial.

6.4 Está terminantemente prohibido editar o alterar grabaciones, excepto para mejorar la calidad con fines de investigación o para difuminar rasgos (pixelado).

6.5 Se autoriza el difuminado de rostros de no participantes en un incidente por motivos de privacidad al entregar imágenes a terceros.

6.6 Los sistemas se configurarán para evitar que los operadores manipulen o dupliquen la información grabada.

6.7 El almacenamiento y acceso serán controlados por el sector de Seguridad Laboral.

6.8 Las grabaciones usadas en procesos judiciales se retendrán hasta la finalización del proceso y el periodo de apelación. La transmisión por red utilizará tecnología de cifrado (encriptación).

7. GESTIÓN DE ACCESO Y MONITOREO

7.1 El acceso a vídeo en vivo o grabado se limita al sector de seguridad y personal designado. La copia o retransmisión requiere autorización previa del gestor del **SECTOR DE TECNOLOGÍA**. Toda información es confidencial.

7.2 La eliminación de vídeos debe ser aprobada por el SECTOR DE TECNOLOGÍA, siguiendo las orientaciones del Delegado de Protección de Datos (DPO).

7.3 Se mantendrá un registro (log) de todos los accesos con fecha e identificación de la persona autorizada.

7.4 El registro de acceso a los datos se mantendrá por un periodo mínimo de 12 meses.

7.5 Las solicitudes de acceso por parte del Titular de los Datos u otros deben fundamentarse en un interés específico y en las hipótesis legales de la LGPD, previa verificación de identidad.

7.6 Las solicitudes internas de otros departamentos deberán dirigirse por escrito al SECTOR DE TECNOLOGÍA para su análisis y aprobación junto con el DPO.

7.7 Las solicitudes externas dirigidas a FLASH ENGENHARIA deberán someterse formalmente al **DEPARTAMENTO JURÍDICO** y al DPO.

7.8 Las demandas legales (citaciones, mandatos de registro) serán gestionadas por el **DEPARTAMENTO JURÍDICO**.

7.9 Para ejercer derechos de acceso, rectificación o exclusión de datos personales del CCTV, el titular debe dirigirse al correo: **lgpd@flashengenharia.com.br**.

8. ÚLTIMA ACTUALIZACIÓN Y VERSIONES ANTERIORES

La última actualización de esta Política de CCTV se realizó el **16 de diciembre de 2025**.