

PROGRAMA DE ADEQUAÇÃO LEI GERAL DE PROTEÇÃO DE DADOS



POLÍTICA DE USO DE CÂMERAS

1. INTRODUÇÃO

A tecnologia do Circuito Fechado de Televisão (CFTV) se desenvolveu nos últimos anos para ser mais confiável, econômico e disponível. Quando usado adequadamente, o CFTV pode ajudar a reduzir o risco de acesso não autorizado às instalações, tranquilizar os usuários e fornecer um registro preciso do que aconteceu quando da ocorrência de um incidente.

A fim de proteger seus usuários, funcionários e outras partes interessadas, a **FLASH ENGENHARIA** faz uso do CFTV em circunstâncias apropriadas para abordar áreas específicas de risco. Ao coletar e usar esses dados de vídeo gravados a **FLASH ENGENHARIA** está sujeito a uma variedade de leis, incluindo a Lei 13.709/18 - Lei Geral de Proteção de Dados (LGPD), que controla como tais atividades podem ser realizadas e as proteções que devem ser postas em prática para proteger os dados de vídeos registrados.

O objetivo desta política é definir as regras que devem ser seguidas, para que as responsabilidades da **FLASH ENGENHARIA** sejam atendidas em todos os momentos e a utilidade dos dados gravados seja conforme determinação legal.

2. OBJETIVO

2.1 Os equipamentos utilizados no sistema de CFTV são para a segurança dos seus colaboradores, usuários, fornecedores e visitantes em geral, bens e informações, visando a prevenção de furtos, prática de assédio sexual e riscos relacionados à segurança interna. A utilização destes equipamentos para dissuasão, poderá incorrer em instauração de investigação e potencial processo criminal por comportamento suspeito e/ou criminoso.

2.2 A empresa **FLASH ENGENHARIA**, inscrita sob o CNPJ Nº 04.844.206/0001-59, com sede na Rua Professora Celia Cangro Marques Mendes, nº 1000 - Alto da Boa Vista - Sorocaba, SP - CEP 18.087-171, opera um sistema de proteção de vídeo monitoramento em toda sua instalação, com a finalidade restrita da promoção da segurança e proteção corporativa de nossa Empresa e necessidades aqui explicitadas, relativo a proteção das pessoas naturais, no que diz respeito ao tratamento dos dados pessoais gravados em formato de imagem, aderentes com a Lei n. 13.709 (Lei Geral de Proteção de Dados), com a portaria Nº 3.233/2012/DG/DPF (Instruções Segurança Privada), Constituição da República Federativa do Brasil de 1988 Art. 5º, e CLT das Leis do Trabalho, contando assim também, com orientações e recomendações emanadas pela ANPD (Autoridade Nacional de Proteção de Dados).

2.3 Esta política não aborda o uso de tecnologia especializada, como Reconhecimento Automático de Placas de identificação, reconhecimento facial ou veículos operados remotamente (drones, também conhecidos como sistemas aéreos não tripulados - VANT).

2.4 Esta política aplica-se a todas as operações, pessoas e processos que constituem os sistemas de segurança da informação da **FLASH ENGENHARIA**, incluindo membros do conselho, diretores, funcionários, fornecedores e outros terceiros, que eventualmente legitimados por outra base legal, possam ter acesso ao sistema de CFTV.

3. PROTEÇÃO DE DADOS

3.1 O sistema de proteção de vídeo monitoramento da **FLASH ENGENHARIA**, tem um propósito específico e legítimo que atende a necessidade ou uma área de risco, como a

prevenção ou redução de crimes em um local que eventualmente possa estar sujeito a atividades ilegais.

3.2 Conforme o princípio de minimização de dados na LGPD, a gravação de vídeo deve estar ativa apenas nos dias e entre os momentos em que é necessária, e a gravação de áudio somente será utilizada quando justificada, levando em consideração as preocupações com privacidade. Para fins de proteção de dados, a **FLASH ENGENHARIA** atuará como a controladora de dados para o uso do CFTV e, quando necessário, registrará com a autoridade fiscalizadora.

3.3 Quando usado um terceiro como parte do tratamento de imagens do CFTV (por exemplo, para armazenamento ou manutenção), ele será considerado um operador no contexto da LGPD e um contrato, tendo seu objeto aderência com o produto e deve estar vigente para este tratamento.

3.4 Para cada implementação de um novo dispositivo de CFTV, deverá ser realizada uma reavaliação no impacto de proteção de dados, considerando os novos riscos, caso existam, aos direitos e liberdades do titular dos dados e garantir que haja proteção adequada. A avaliação de impacto de proteção de dados deve ser revisada regularmente e mediante mudanças significativas que possam afetar suas conclusões. A hipótese legal para tratamento de dados de imagem pelo CFTV é a promoção da segurança e proteção corporativa da **FLASH ENGENHARIA**, conforme os avisos publicados em cada setor/área/sala onde estão instaladas as câmeras.

3.5 A **FLASH ENGENHARIA**, procederá anualmente uma revisão e avaliação da conformidade da presente política com as regras em matéria de proteção de dados e privacidade ou sempre que houver qualquer revisão ou atualização.

4. ESPAÇOS COBERTOS

4.1 De acordo com o objetivo descrito no item 1 desta política, a inserção de câmeras levou em conta a necessidade de manter um perímetro de segurança e de controlar os acessos a partir do exterior, de modo que esteja adequado às circunstâncias do local e de modo que não restrinja ou viole os direitos dos cidadãos. As áreas de cobertura englobam todo o espaço físico interno e externo sob responsabilidade da **FLASH ENGENHARIA**, não necessariamente sendo focada diretamente ao colaborador, o que estaria violando sua privacidade conforme Art. 5º inciso X.

4.2 As câmeras como citado no tópico acima, estão localizadas interna e externamente, e em diferentes pontos da **FLASH ENGENHARIA** sejam eles: galpões produtivos, perímetro externo, portarias, dentre outros. A inserção nestes locais, foi cuidadosamente analisada para garantir a minimização da coleta e a vigilância dos espaços que não são relevantes para os fins previstos.

5. SINALIZAÇÃO

5.1 Os locais que contenham dispositivo de vigilância por vídeo deverão ser obrigatoriamente sinalizados com avisos ou placas. O texto que constará do aviso ou placa deverá ser compatível com o que estabelece o princípio da transparência definido na LGPD.

6. ARMAZENAMENTO E RETENÇÃO

6.1 A limitação de armazenamento das imagens será de no mínimo 7 dias e no máximo 45 dias, ou ainda a capacidade que o hardware suportar (dispositivo de gravação de imagens).

6.2 O Armazenamento deverá ser mantido em um local seguro com acesso apenas ao pessoal autorizado. As mídias serão guardadas e transportadas de maneira a preservar a segurança. As mídias atuais e arquivadas devem ser mantidas trancadas e protegidas.

6.3 Toda(s) a(s) gravação(ões) realizada(s) como “registros de vigilância” por vídeo, deverá(ão) ser retida(s) em armazenamento local seguro por um período não superior a 02 (dois) anos. Após esse período, as gravações deverão ser apagadas ou sobrescritas, a menos que retidas como parte de uma investigação criminal ou processo judicial (criminal ou civil).

6.4 É terminantemente proibido editar, alterar ou interceptar gravações ou imagens estáticas, exceto para melhorar a qualidade para fins de investigação ou desfocar recursos. Nenhuma tentativa deve ser permitida para alterar qualquer parte de qualquer gravação de vigilância.

6.5 A única exceção autorizada será a ação de desfocar rostos de não participantes em um incidente por motivos de privacidade no caso de um vídeo ou imagem estática ser fornecida à terceiros. Devem ser tomadas medidas para garantir que nenhuma edição ou alteração comprometa o vídeo gravado.

6.6 Os sistemas de vigilância e monitores deverão ser configurados para evitar que os operadores das câmeras de segurança adulterem ou dupliquem as informações gravadas.

6.7 As gravações serão armazenadas de maneira consistente com a tecnologia disponível e transportadas de maneira a preservar a segurança. As gravações atuais e arquivadas serão protegidas. Todo o armazenamento e acesso às gravações serão controlados pelo setor de segurança do trabalho. Os registros de vigilância não devem ser armazenados por outros departamentos.

6.8 As gravações usadas em investigações de aplicação da lei ou processos criminais devem ser retidas até o final do processo judicial e período de apelação, a menos que seja instruído de outra forma por um tribunal. As gravações também deverão ser retidas por outros motivos de boa-fé, conforme determinado pelo departamento Jurídico da empresa. A transmissão de gravações pela Internet ou rede da empresa deverá usar tecnologia de criptografia para garantir que as gravações não sejam acessadas indevidamente

6.9 Toda(s) a(s) gravação(ões) realizada(s) como “registros de vigilância” por vídeo, deverá(ão) ser retida(s) em armazenamento local seguro por um período não superior a 02 (dois) anos. Após esse período, as gravações deverão ser apagadas ou sobrescritas, a menos que retidas como parte de uma investigação criminal ou processo judicial (criminal ou civil).

7. GESTÃO DE ACESSO E MONITORAMENTO

7.1 O acesso ao vídeo ao vivo ou ao vídeo gravado das câmeras deve ser limitado ao setor de segurança e pessoal designado. A cópia, duplicação e/ou retransmissão de vídeo ao vivo ou gravado deve ser limitada a pessoas autorizadas previamente pelo gestor do SETOR DE TECNOLOGIA. Os funcionários da **FLASH ENGENHARIA** estão proibidos de usar ou divulgar informações adquiridas das câmeras de segurança, exceto para fins oficiais. Todas as informações e/ou observações feitas no uso de câmeras de segurança são consideradas confidenciais e só podem ser usadas para fins oficiais da empresa e de aplicação da lei.

7.2 A exclusão de vídeo, de acordo com esta política, e qualquer isenção à Política de Retenção e Destruição de Dados deve ser aprovada pelo SETOR DE TECNOLOGIA, seguindo as orientações do Encarregado de Dados (DPO). Apenas o SETOR DE TECNOLOGIA deverá ter permissão para excluir gravações de vídeo de acordo com esta política.

7.3 O SETOR DE TECNOLOGIA deve manter um registro de todas as instâncias de acesso ou uso de registros de vigilância. O registro deve incluir a data e a identificação da pessoa ou pessoas a quem o acesso foi concedido. O setor de segurança também manterá uma lista de pessoal aprovado para monitorar feeds de vídeo ao vivo e/ou gravados. As gravações não relacionadas a, ou usadas para uma investigação, devem ser mantidas em sigilo e os dados deverão ser destruídos ao serem sobrescritos.

7.4 Um registro que documente o acesso e o uso dos dados armazenados no sistema de vigilância centralizado da empresa deverá ser mantido por um período de, no mínimo, 12 (doze) meses.

7.5 Nas solicitações de acesso, na obtenção das imagens do CFTV, realizadas pelo Titular de Dados ou demais solicitações, estas deverão ser fundamentadas em interesse específico, demonstrada a pertinência do pedido e lastreados nas hipóteses legais previstas na LGPD, onde será incluída todas as verificações necessárias para averiguar o direito legal de acesso e a identidade do solicitante. Quando aprovada nos termos acima, as imagens gravadas podem ser visualizadas (sujeitas a controles de acesso) ou um registro das imagens pode ser fornecido.

7.6 Para as solicitações provenientes de fontes internas, (Departamentos, Áreas, Unidades ou Setores) da **FLASH ENGENHARIA** que necessitem ter acesso a vídeos ao vivo e/ou gravados deverão encaminhar uma solicitação por escrito ao SETOR DE TECNOLOGIA, com o conhecimento prévio da Empresa Controladora, descrevendo a necessidade e justificativa, e o SETOR DE TECNOLOGIA com o conhecimento do DPO analisará a solicitação e aprovará ou não o pedido feito.

7.7 As solicitações de fontes externas direcionadas ao Controlador **FLASH ENGENHARIA**, para a liberação de dados de vídeos gravados, obtidos por meio de monitoramento de vigilância ou gravação, deverão ser submetidas previamente e formalmente ao DEPARTAMENTO JURÍDICO e conhecimento do DPO da **FLASH ENGENHARIA**, para aprovação antes da liberação.

7.8 Solicitações referentes ao atendimento de demandas legais (Intimações, Mandados de busca e apreensão etc.) para liberação de dados de vídeos gravados deverão ser encaminhados ao DEPARTAMENTO JURÍDICO e levado ao conhecimento do DPO quando aplicável, da **FLASH ENGENHARIA**. Caberá ao DEPARTAMENTO JURÍDICO da **FLASH ENGENHARIA** revisar e responder a todas as intimações de aplicação da lei para liberar as gravações obtidas por meio de monitoramento de vídeo e CFTV.

7.9 Para o titular de dados exercer algum pedido de acesso, retificação, bloqueio e/ou exclusão de dados pessoais resultantes do uso do CFTV devem ser encaminhados para o endereço de e-mail: lgpd@flashengenharia.com.br.

8. ÚLTIMA ATUALIZAÇÃO E VERSÕES ANTERIORES

A última atualização desta Política de CFTV foi realizada em 16 de dezembro de 2025.