

POP

HC-UFTM/EBSERH

Utilização da Sala de Videomonitoramento e Disponibilização de Imagens

Versão: 4 | 2026

SUPERINTENDENTE

LUCIANA DE ALMEIDA SILVA TEIXEIRA

GERENTE ADMINISTRATIVO

RODRIGO JULIANO MOLINA

CHEFE DA DIVISÃO DE LOGÍSTICA E INFRAESTRUTURA HOSPITALAR

ÁLVARO APARECIDO SANTIAGO

CHEFE DA UNIDADE DE SUPORTE OPERACIONAL

EURÍPEDES ROGÉRIO DOS SANTOS CAMILO

ELABORAÇÃO DA VERSÃO ATUAL

Eurípedes Rogério dos Santos Camilo, Unidade de Suporte Operacional

REGISTRO, VALIDAÇÃO DE FORMA E REVISÃO

Ana Paula Corrêa Gomes, Comissão de Gestão da Qualidade Documental

APROVAÇÃO

Álvaro Aparecido Santiago, Divisão de Logística e Infraestrutura Hospitalar

Data da emissão: 8/4/2026

Vigência: dois anos

Código do documento: POP.HC-UFTM-USOP.005

ISBN:

Cópia eletrônica não controlada. Permitida a reprodução parcial ou total, desde que indicada a fonte e sem fins lucrativos. O uso deste documento em meio físico ou fora da vigência pode disseminar informação e/ou procedimento desatualizados © 2026, Empresa Brasileira de Serviços Hospitalares. Todos os direitos reservados www.ebserh.gov.br



Hospital de Clínicas



1. OBJETIVO

Este Procedimento Operacional Padrão (POP) foi elaborado com o intuito de formalizar a padronização do fluxo de trabalho e das atividades da Sala de Videomonitoramento do Hospital de Clínicas da Universidade Federal do Triângulo Mineiro (HC-UFTM), bem como relacionar os procedimentos necessários à operacionalização do local.

2. GLOSSÁRIO

CFTV – Circuito Fechado de TV

DVR – Digital Video Recorder

EBSERH – Empresa Brasileira de Serviços Hospitalares

HC-UFTM – Hospital de Clínicas da Universidade Federal do Triângulo Mineiro

NVR – Network Video Recorder

POP – Procedimento Operacional Padrão

SEGOV – Setor de Governança e Estratégia

SV – Sala de Videomonitoramento

USOP – Unidade de Suporte Operacional

3. SALA DE VIDEOMONITORAMENTO (SV)

A Sala de Videomonitoramento está subordinada diretamente à Unidade de Suporte Operacional (USOP) e tem por finalidade o assessoramento técnico e operacional relativo à segurança institucional. Suas atividades abrangem tanto as áreas internas quanto às externas do HC-UFTM e de suas unidades anexas, utilizando um sistema de câmeras de vigilância eletrônica estrategicamente posicionadas em diversos pontos do complexo hospitalar. Esse monitoramento possibilita a observação remota e constante de áreas sensíveis, além de ampliar a vigilância em locais onde a presença física das equipes do HC-UFTM não é total, assegurando uma cobertura completa e eficiente das dependências da instituição.

A Sala de Videomonitoramento será diretamente responsável por armazenar, catalogar e controlar as imagens captadas pelos softwares de segurança eletrônica, assumindo também o papel de fornecer os registros e arquivos de situações ou eventos relevantes. Essas gravações têm como objetivo esclarecer fatos ocorridos dentro das dependências do HC-UFTM e de seus anexos, fornecendo subsídios que permitam uma tomada de decisão mais fundamentada e precisa por parte dos gestores de cada Unidade ou Setor, bem como por outras autoridades competentes.

As Unidades e Setores terão a função de identificar e listar pessoas, veículos e outros materiais ou equipamentos que necessitem de acompanhamento ou de investigação preliminar por parte de comissões internas e autoridades competentes. Essa atribuição tem como objetivo central garantir a segurança de toda a instituição, bem como proteger os usuários que utilizam os serviços oferecidos pelo hospital.

O videomonitoramento será realizado por câmeras de segurança instaladas nas edificações do complexo hospitalar e conectadas a dispositivos digitais de gravação (DVRs ou NVRs), que permitem o armazenamento das imagens tanto nos discos rígidos dos próprios equipamentos quanto no servidor do HC-UFTM.

A Sala de Videomonitoramento realizará o acompanhamento de todo o complexo hospitalar. A USOP e o Setor de Tecnologia da Informação e Saúde Digital (SETISD) deverão propor

ações que viabilizem a ampliação do sistema e a instalação de novos equipamentos e tecnologias de segurança.

4. CONCEITOS

Circuito Fechado de TV (CFTV): refere-se ao componente do sistema de segurança eletrônica composto por câmeras que transmitem imagens de pontos estratégicos para uma central de monitoramento. Esse sistema permite o acompanhamento em tempo real, viabilizando uma resposta imediata em caso de intercorrência ou situação de risco.

Credenciamento: é o processo de habilitação do operador, por meio do qual ele recebe as credenciais necessárias para acessar o sistema. Esse procedimento inclui a identificação formal do profissional e a definição do seu perfil de acesso aos recursos de monitoramento.

Credenciais de acesso: são as permissões de acesso ao sistema de videomonitoramento concedidas pelo responsável pela Sala de Videomonitoramento que autorizam o operador a utilizar as informações ou recursos do local.

Perfil de acesso: define o conjunto de permissões e ferramentas que cada operador pode utilizar, estabelecido previamente de acordo com as necessidades e responsabilidades de sua função no sistema.

Coordenador: é o agente público com autoridade para realizar e autorizar modificações, permanentes ou temporárias, nas configurações de programas e dispositivos. Além disso, cabe ao coordenador a função de fiscalizar e supervisionar as atividades realizadas pelos operadores.

Operador: é o profissional encarregado do acompanhamento diário e contínuo do sistema de segurança eletrônica, zelando pela vigilância das imagens.

Usuário: refere-se a qualquer pessoa que, embora não faça parte da equipe de videomonitoramento, recebeu autorização para acessar o sistema em casos específicos.

5. DISPOSIÇÕES PRELIMINARES

O operador deve zelar pela integridade de todas as informações obtidas por meio dos Sistemas de Segurança Eletrônica durante o exercício de suas funções, assumindo a responsabilidade direta pelo armazenamento adequado, pela transmissão segura e pela total confidencialidade desses dados.

É vedado o acesso, o armazenamento, a transmissão ou o transporte de qualquer conteúdo que seja considerado incompatível com os princípios da moralidade administrativa, com as obrigações do cargo ou com as diretrizes estabelecidas pela Política de Segurança Institucional.

É vedada a prática de qualquer ação que tenha o objetivo intencional de comprometer a segurança do sistema, o funcionamento dos equipamentos de CFTV ou a proteção das informações armazenadas nesses dispositivos.

6. COMPETÊNCIAS DAS EQUIPES DA SALA DE VIDEOMONITORAMENTO

Administração de Informações: administrar as informações geradas pelo Sistema de Monitoramento, atuando em conjunto com a USOP para garantir o cumprimento das normas de segurança institucional. Essa atribuição inclui o gerenciamento e a fiscalização constante de todas as atividades de videomonitoramento realizadas nas dependências do complexo hospitalar.

Registro e Controle de Eventos: gerar e controlar os registros de todos os eventos relevantes que ocorram nas áreas internas e externas do complexo hospitalar, sendo responsável pela elaboração e pelo envio de relatórios e comunicados internos à USOP.

Gestão de Imagens e Dados: manter o controle exclusivo sobre o armazenamento e a disponibilização das imagens captadas e gravadas pelos Sistemas de Monitoramento. Essa exclusividade visa assegurar a proteção total dos dados e garantir que todos os procedimentos de gestão da informação ocorram dentro da legalidade.

Acompanhamento Técnico: realizar o acompanhamento contínuo e a produção de relatórios detalhados sobre todos os serviços e atividades executados dentro de sua área de competência técnica e operacional.

Processamento e Comunicação: processar integralmente as imagens e informações coletadas, tendo a obrigação de comunicar à USOP qualquer irregularidade detectada, especialmente em casos de interrupções, totais ou parciais, no funcionamento dos Sistemas de Monitoramento.

7. EQUIPE DA SALA DE VIDEOMONITORAMENTO

A equipe da Sala de Videomonitoramento será constituída por encarregados do serviço de portaria, devidamente qualificados, na quantidade mínima de 1 (um) operador por turno de trabalho.

Os profissionais supracitados receberão treinamento específico sobre a operação dos equipamentos e as responsabilidades inerentes ao operador do Sistema de Segurança Eletrônica. Essa capacitação abrangerá temas fundamentais, como os níveis de classificação da informação e a identificação de tipos de ocorrências, além de esclarecer as penalidades administrativas aplicáveis em caso de condutas inadequadas previstas neste procedimento, sem prejuízo das sanções de natureza civil e penal que possam ser cabíveis.

8. COORDENAÇÃO DA EQUIPE

O coordenador da equipe, profissional com experiência comprovada em segurança eletrônica, será designado pela chefia da USOP para prestar assessoramento técnico e exercer as seguintes atribuições:

- **Gerir a equipe e os serviços:** coordenar as atividades operacionais e garantir a qualidade e eficiência do monitoramento.
- **Proteger dados:** zelar pela segurança e pelo sigilo das imagens e informações do sistema.
- **Reportar à USOP:** informar fatos relevantes e irregularidades, enviando relatórios estatísticos e registros de ocorrências.
- **Gerenciar acessos:** cadastrar operadores, manter dados atualizados e controlar a habilitação ou desativação de senhas.
- **Fiscalizar a conduta:** garantir o cumprimento das normas de monitoramento e verificar se a postura dos operadores é adequada à função.
- **Atualizar normas e tecnologias:** manter-se atualizado sobre as instruções de segurança e ministrar treinamentos para novos operadores ou novas tecnologias.

9. ATRIBUIÇÕES DOS OPERADORES

Constituem deveres e responsabilidades dos operadores as diretrizes e condutas listadas a seguir, visando a segurança, o sigilo e a integridade operacional do Sistema de Videomonitoramento:

- **Operação e Zelo Técnico:** operar o Sistema de Monitoramento com esmero, habilidade e perícia, abstendo-se de explorar falhas, vulnerabilidades ou utilizar ferramentas para obter dados de autenticação de usuários.

- **Inspeção e Manutenção:** realizar inspeção de segurança no início do turno em todo o sistema e instalações, registrando e comunicando irregularidades para solução imediata. É vedado o manuseio de líquidos ou alimentos próximo aos equipamentos.
- **Vigilância Ativa:** acompanhar o monitoramento e o sistema de gravação para alertar profissionais de portaria/vigilância sobre atitudes suspeitas, sinistros, irregularidades ou comportamentos inadequados.
- **Gestão de Dados e Mídias:** realizar backup de imagens e, quando expressamente autorizado, gravar arquivos em mídias externas. É proibido conectar componentes externos (modem, pendrive, HD etc.) sem autorização formal específica.
- **Sigilo e Ética:** manter discricção absoluta sobre o que for observado, sendo vedados comentários ou especulações. Deve-se respeitar os direitos de imagem e propriedade intelectual, em conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD), nº 13.709/2018).
- **Segurança de Acesso:** manter credenciais e senhas em sigilo absoluto, respeitando os limites de autorização da conta e as condições expressas no Termo de Responsabilidade.
- **Integridade do Sistema:** não interferir, interromper ou burlar a operação normal da rede e dos mecanismos de proteção de ativos (computador, terminal, rack etc.).
- **Controle e Acesso à Sala:** zelar pela carga patrimonial da Sala de Videomonitoramento e impedir o acesso de pessoas não autorizadas ao local ou aos sistemas, sob pena de corresponsabilidade por eventuais problemas disso decorrentes.
- **Registros Administrativos:** preencher relatório de ocorrências detalhando eventos, procedimentos, tarefas agendadas e demais anotações relevantes para a coordenação.

10. FORNECIMENTO DE IMAGENS E DE INFORMAÇÕES

A Sala de Videomonitoramento fornecerá imagens e informações mediante solicitação formal via Sistema Eletrônico de Informações (SEI), endereçada à Superintendência do HC-UFTM, autoridade competente para autorizar ou indeferir a disponibilização do material gravado.

Procedimentos de Solicitação

- **Usuários Internos:** devem realizar a solicitação por meio de processo SEI sigiloso direcionado à Superintendência para os trâmites de análise e autorização.
- **Usuários Externos:** devem encaminhar um e-mail ao Setor de Governança e Estratégia (SEGOV), que procederá com a abertura do processo SEI sigiloso e o encaminhamento para os trâmites de análise e autorização da Superintendência.
- ✓ Em conformidade com a LGPD, toda solicitação deverá obrigatoriamente conter:
 - Nome completo e número de documento individual do solicitante (e, quando aplicável, da pessoa formalmente autorizada por ele);
 - Descrição sucinta das informações solicitadas e a justificativa da necessidade;
 - Destinação final do material;
 - Outras informações julgadas relevantes diante das peculiaridades do caso concreto.

Fluxo de Atendimento e Disponibilização

Após a análise e eventual autorização da Superintendência, o processo será encaminhado à USOP. Esta, por sua vez, repassará a demanda à equipe de videomonitoramento para a realização do backup dos arquivos, que serão devolvidos à USOP.

De posse dos arquivos, a USOP gerará um link para acesso e download, disponibilizando-o ao solicitante conforme os termos da autorização concedida.

Nota sobre prazos: o link permanecerá ativo por 15 dias corridos. Após esse período, a USOP desativará o acesso e excluirá os arquivos contidos, não se responsabilizando por eventuais perdas decorrentes da não realização do download dentro do prazo estabelecido.

Segurança e Sigilo

Apenas operadores devidamente autorizados pela USOP possuem legitimidade para copiar imagens e realizar procedimentos técnicos de manuseio do material. Todo o serviço deve ser rigorosamente registrado e documentado.

Os operadores envolvidos devem prezar pelo sigilo absoluto das informações de caráter restrito. O material somente sairá da Sala de Videomonitoramento mediante autorização expressa da USOP ou da autoridade competente.

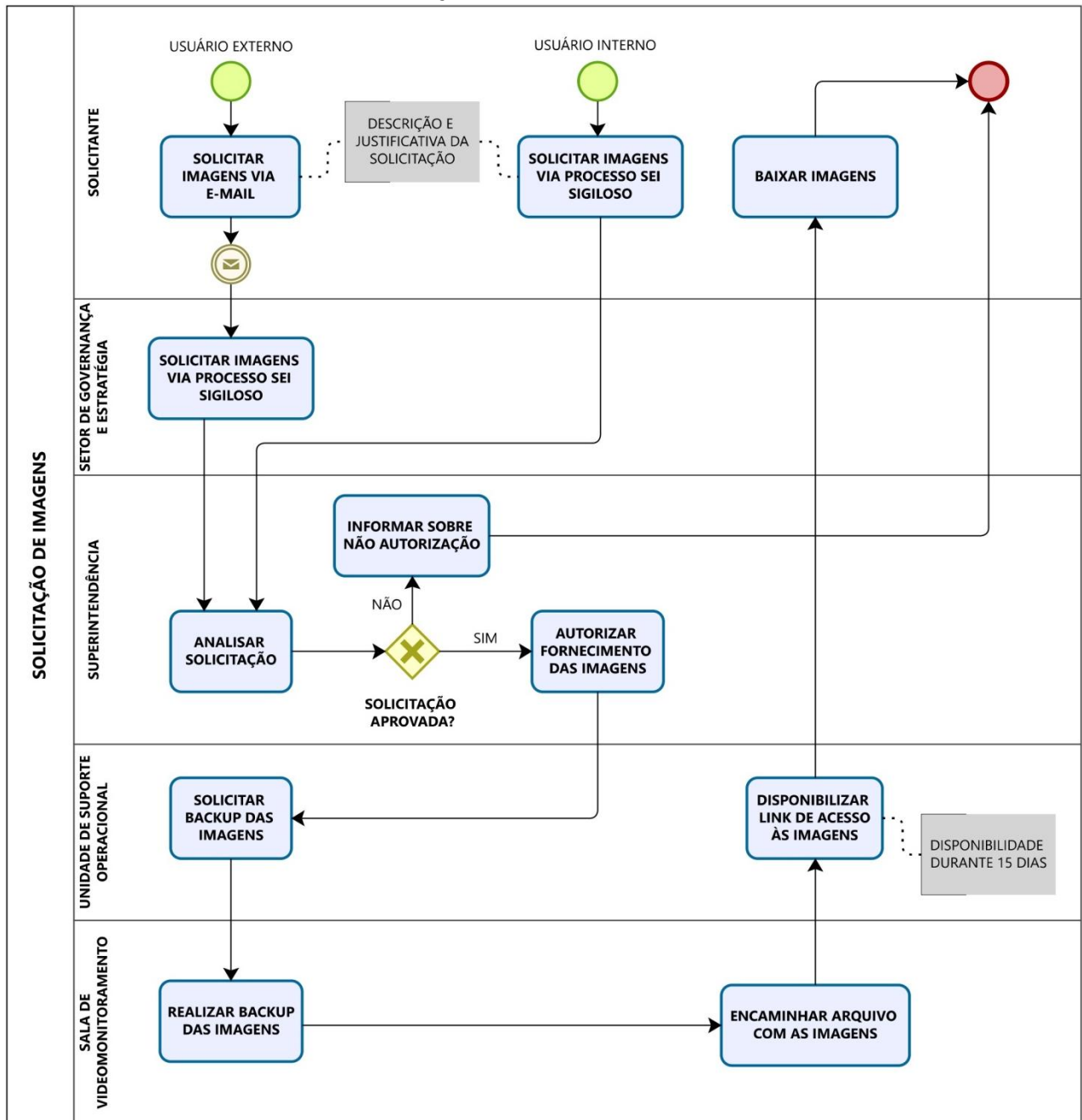
Os operadores devem zelar pelo sigilo absoluto das informações de caráter restrito, sendo que o material captado somente poderá sair da Sala de Videomonitoramento mediante autorização expressa da USOP ou da autoridade competente. É terminantemente vedada a realização de backups ou a veiculação de imagens por meio de celulares, pendrives ou quaisquer outras mídias externas. Todos os procedimentos devem ser realizados estritamente conforme os termos deste POP e mediante as devidas autorizações.

Critérios de Acesso

O acesso às imagens e informações será permitido exclusivamente para:

1. Atendimento, na forma da lei, a necessidades de investigação administrativa ou criminal;
2. Atendimento ao interesse público;
3. Cumprimento de ordem da Superintendência do HC-UFTM (ou servidor por ela designado) e demais situações previstas neste POP.

11. FLUXOGRAMA DA DISPONIBILIZAÇÃO DE IMAGENS



12. NÍVEIS DE CLASSIFICAÇÃO DA INFORMAÇÃO

A classificação da informação gerada pelo Sistema de Videomonitoramento é estipulada pela chefia da USOP e divide-se nos seguintes níveis:

- **Nível de alto risco:** compreende informações estratégicas, confidenciais e de sigilo absoluto, sendo rigorosamente protegidas contra qualquer acesso externo.
- **Nível de uso restrito:** engloba informações destinadas a áreas ou grupos específicos de pessoas, possuindo um caráter confidencial de menor risco.

- **Nível de uso interno:** abrange informações voltadas a gestores, servidores e empregados. O acesso externo deve ser evitado, embora um eventual vazamento ao público não acarrete consequências críticas.
- **Nível de uso público:** refere-se a informações direcionadas a outros órgãos públicos, fornecedores e terceiros. Por serem de livre acesso, não demandam sigilo ou investimento de recursos para sua proteção.

13. CICLO DE VIDA DA INFORMAÇÃO

O ciclo de vida da informação é composto pelos momentos em que os dados são processados e, conseqüentemente, expostos a riscos. Esses estágios compreendem:

- **Manuseio da informação:** ocorre no momento de sua criação ou manipulação, como no uso de senhas para deferimento e autenticação, ou durante a digitação de novos dados gerados.
- **Armazenamento da informação:** refere-se ao estágio em que os dados são guardados, seja em mídias físicas ou em bancos de dados compartilhados.
- **Transporte da informação:** consiste na distribuição ou envio de dados, abrangendo desde comunicações via rádio ou telefone institucional sobre temas confidenciais até a postagem de documentos ou o encaminhamento por correio eletrônico (e-mail).
- **Descarte da informação:** etapa final em que a informação é excluída após a perda de sua utilidade, seja pela deleção de arquivos digitais ou pelo descarte físico de documentos impressos.

14. DIRETRIZES DE ARMAZENAMENTO E SEGURANÇA

As cópias de segurança e o armazenamento de dados institucionais devem seguir as seguintes normas de proteção e continuidade:

- **Gestão de Cópias de Segurança (Backup):** as cópias de segurança devem ser armazenadas em ambientes seguros, restritos e distintos da localização das informações originais, utilizando dispositivos que minimizem a exposição e o manuseio das mídias. Para garantir a continuidade em casos de contingência, devem-se manter cópias de todos os dados necessários à manutenção em locais alternativos. Sempre que a criticidade da informação exigir, uma cópia de segurança adicional deve ser efetuada e guardada em local distinto.
- **Armazenamento de Dados Institucionais:** arquivos digitais de interesse do HC-UFTM deverão ser armazenados nos servidores da instituição ou em local determinado pela Superintendência, com o devido registro de recebimento pelo responsável designado. Caso seja necessário o armazenamento em estações de trabalho, a guarda dos dados ficará sob responsabilidade direta dos operadores.
- **Restrições e Vedações:** é terminantemente proibido o armazenamento de dados pessoais na infraestrutura da Sala de Videomonitoramento.
- **Responsabilidades da Equipe:** cabe à equipe responsável definir e disponibilizar a estrutura necessária (volume, armazenamento e tempestividade) para a execução dos serviços, além de certificar-se da compatibilidade entre as versões de *softwares* utilizados na geração e restauração das cópias de segurança.

15. GESTÃO DO SISTEMA DE SEGURANÇA ELETRÔNICA

O chefe da USOP atuará como gestor do Sistema de Segurança Eletrônica, competindo-lhe as seguintes atribuições:



Hospital de Clínicas



- **Controle de Acessos e Perfis:** definir formalmente os perfis de acesso às instalações, equipamentos, ações e materiais desenvolvidos, além de estabelecer e atribuir as restrições de acesso para cada unidade organizacional.
- **Gestão de Credenciais e Operações:** determinar quais operações exigem o uso de senhas e definir os níveis operacionais vinculados às equipes de videomonitoramento, mantendo atualizada a relação de liberações de uso.
- **Classificação e Monitoramento:** estabelecer o nível de classificação das operações dos aplicativos, conforme as normas de classificação da informação, e monitorar continuamente o uso dessas ferramentas.
- **Auditoria e Conformidade:** definir e implementar registros de auditoria para as operações dos aplicativos, determinando seus respectivos prazos de retenção.
- **Transparência e Controle:** autorizar o fornecimento de informações relativas aos registros de auditoria das operações e auditar regularmente as utilizações do sistema.

16. CONTROLE DE ACESSO

O acesso ao sistema e aos equipamentos de segurança eletrônica do HC-UFTM é restrito ao cabeamento estruturado próprio, sob supervisão e seguindo os procedimentos e mecanismos definidos pelo SETISD.

Requisitos para Criação de Contas

A concessão de acesso aos ativos do CFTV exige autorizações específicas:

- **Profissionais Terceirizados:** autorização da chefia da USOP;
- **Representantes de outros órgãos públicos:** autorização da Superintendência do HC-UFTM.

As credenciais de acesso às contas individuais são estritamente únicas, pessoais e intransferíveis.

Responsabilidades da USOP

Compete à USOP a gestão administrativa dos acessos, incluindo:

- **Manutenção Cadastral:** manter atualizados os dados dos profissionais que exercem funções de administração do sistema;
- **Procedimentos de Acesso:** estabelecer fluxos auditáveis para o credenciamento, bloqueio e exclusão de contas de usuários;
- **Rastreabilidade:** registrar todos os acessos à rede do CFTV, garantindo a identificação de administradores e usuários por um período mínimo de 2 (dois) anos.

Política de Senhas

As senhas de acesso aos ativos de informação cadastradas pelos administradores devem observar os seguintes critérios de segurança:

- **Composição:** mínimo de 8 (oito) caracteres, com combinação obrigatória de letras, números e caracteres especiais;
- **Validade:** a troca deve ocorrer em um período de até 180 (cento e oitenta) dias. O sistema notificará o usuário sobre a expiração da senha ao final deste prazo.

17. MANUTENÇÃO E SUPORTE TÉCNICO

As diretrizes para a preservação e o suporte técnico dos ativos do Sistema de Segurança Eletrônica são as seguintes:



Hospital de Clínicas



- **Abertura de Chamados:** toda solicitação de suporte ou manutenção em equipamentos e sistemas deve ser realizada pelos operadores, sob a supervisão direta e o direcionamento da USOP.
- **Restrições de Intervenção:** é estritamente vedada qualquer intervenção, manuseio físico ou abertura de equipamentos do sistema sem o prévio conhecimento e autorização da USOP.
- **Controle de Software:** é proibida a instalação ou o uso de quaisquer aplicativos e sistemas operacionais nos equipamentos da Sala de Videomonitoramento que não tenham sido expressamente definidos ou autorizados pela USOP.
- **Execução de Serviços Externos:** serviços de expansão, atualização, substituição ou manutenção corretiva/preventiva serão executados exclusivamente por empresas contratadas e autorizadas para este fim, ou por profissional técnico formalmente designado.

18. CONSIDERAÇÕES FINAIS

Para o encerramento das diretrizes deste protocolo, estabelecem-se as seguintes condições e normas complementares:

- **Restrição de Acesso:** o acesso e a permanência na Sala de Videomonitoramento são exclusivos aos operadores do sistema, profissionais de manutenção (preventiva e corretiva) e pessoas formalmente autorizadas pela USOP, ressalvados os casos determinados pela Superintendência do HC-UFTM.
- **Continuidade Operacional:** a prestadora de serviços terceirizados, responsável pela equipe de operadores da Sala de Videomonitoramento, deverá manter um cadastro reserva de pessoal habilitado para substituições eventuais, garantindo que a operação do sistema não seja interrompida por afastamentos obrigatórios de operadores.
- **Operação por Terceiros:** profissionais de portaria ou vigilância terceirizados poderão operar os equipamentos para fins de segurança institucional, desde que a atribuição esteja prevista em cláusula contratual e que eles recebam treinamento ministrado por responsáveis designados pela USOP.
- **Uso do Ramal Telefônico:** o ramal da Sala de Videomonitoramento destina-se única e exclusivamente a atividades profissionais. É terminantemente proibido o seu uso para assuntos particulares ou alheios ao interesse institucional que possam comprometer a agilidade dos serviços.
- **Transparência e Sinalização:** avisos informando sobre o monitoramento por meio do Sistema de Segurança Eletrônica deverão ser afixados em locais de fácil visualização.
- **Prazos de Guarda e Sigilo:** as imagens e informações gravadas possuem caráter reservado e devem ser armazenadas com segurança, observando-se os seguintes prazos mínimos de disponibilidade:
 - **Imagens:** 15 (quinze) dias;
 - **Informações:** 06 (seis) meses.

19. REFERÊNCIAS

Diário Eletrônico da Justiça do Trabalho (DEJT) nº 2202, de 04.04.2017, Caderno Administrativo do Tribunal Regional do Trabalho (TRT) da 7ª Região, reservados os direitos autorais.

Lei Geral de Proteção de Dados Pessoais (LGPD) - Lei Nº 13.709, de 14 de agosto de 2018.

https://www.planalto.gov.br/ccivil_03/ato2015-2018/2018/lei/l13709.htm

Acesso em 3/3/2026



Hospital de Clínicas



20. HISTÓRICO DE ELABORAÇÃO/REVISÃO

VERSÃO	DATA	DESCRIÇÃO DA AÇÃO/ALTERAÇÃO
1	27/4/2020	Elaboração da 1ª versão do POP
2	18/5/2022	Revisão do documento
3	1º/4/2024	Revisão do documento
4	8/4/2026	Revisão do documento e inserção em novo modelo

21. RESPONSÁVEIS PELO DOCUMENTO

Elaboração da versão 4 – data: 5/3/2026

Eurípedes Rogério dos Santos Camilo, chefe da Unidade de Suporte Operacional (USOP)

Aprovação – data: 18/3/2026

Álvaro Aparecido Santiago, chefe da Divisão de Logística e Infraestrutura Hospitalar (DLIH)

Registro, validação de forma e revisão – data: 8/4/2026

Ana Paula Corrêa Gomes, coordenadora da Comissão de Gestão da Qualidade Documental

Elaboração da versão 3 – data: 1º/4/2024

Eurípedes Rogério dos Santos Camilo, chefe USG

Validação

Eurípedes Rogério dos Santos Camilo, chefe da USG

Raquel Bessa Ribeiro Rosalino, chefe da Unidade de Gestão da Qualidade e Segurança do Paciente

Registro, análise e revisão

Ana Paula Corrêa Gomes, chefe da Unidade de Planejamento, Gestão de Riscos e Controles Internos (UPLAG)

Aprovação

Carlos Batista Miranda Neto, chefe da DLIH substituto

Elaboração da versão 2 – data: 18/5/2022

Eurípedes Rogério dos Santos Camilo, chefe da Unidade de Serviços Gerais (USG)

Registro, análise e revisão

Maria Aparecida Ferreira, enfermeira da UPLAG

Ana Paula Corrêa Gomes, chefe da UPLAG

Aprovação

Luiz Humberto Camilo, chefe da DLIH

Elaboração da versão 1 – data: 27/4/2020

Renata Maria Dias de Abreu, chefe do Setor de Hotelaria Hospitalar

Eurípedes Rogério dos Santos Camilo, assistente do Setor de Hotelaria Hospitalar

Registro, análise, formatação e revisão

Ana Paula Corrêa Gomes, chefe da Unidade de Planejamento

Validação

Renata Maria Dias de Abreu, chefe do Setor de Hotelaria Hospitalar

Aprovação

Luiz Humberto Camilo, chefe da DLIH substituto