

# SEGURANÇA E CONTROLE DE ACESSO

MANUAL NORMATIVO OPERACIONAL - CLASSIFICAÇÃO #1 - INTERNO

## 1. Finalidade

Este Manual Normativo Operacional regulamenta a aplicação do **MN005.v1 - Segurança e Controle de Acesso**, estabelecendo os mecanismos gerais de controle dos acessos físicos e virtuais às unidades, áreas, ambientes, sistemas, informações e recursos da BrisaLuz AFA.

Os controles destinam-se à proteção das pessoas, instalações, informações e atividades institucionais, assegurando identificação, segurança, rastreabilidade, auditabilidade e prevenção ao desvio de finalidade.

## 2. Princípios gerais

O controle de acesso observará os princípios da identificação, autorização, necessidade, responsabilidade individual, rastreabilidade e proporcionalidade.

Todo acesso deverá guardar relação com a finalidade que justificou sua realização ou autorização.

A autorização para determinado ambiente, unidade, sistema ou recurso não implica autorização automática para os demais.

Os controles poderão combinar mecanismos físicos, eletrônicos, digitais, documentais e humanos.

## 3. Tipos de acesso

**I - acesso físico:** ingresso, circulação ou permanência em unidades, instalações, áreas ou ambientes físicos da BrisaLuz AFA;

**II - acesso virtual:** ingresso, utilização ou permanência em sistemas, plataformas, contas, arquivos, bancos de dados, serviços digitais, **WhatsApp institucional e demais canais institucionais de comunicação**, bem como outros ambientes digitais utilizados pela BrisaLuz AFA.

Os controles de acesso físico e virtual poderão funcionar de maneira independente ou integrada.

## 4. Identificação e responsabilidade individual

Toda pessoa submetida ao controle de acesso deverá utilizar sua própria identificação e os meios de acesso que lhe tenham sido atribuídos.

Credenciais, usuários, senhas, cartões, chaves, códigos, tokens e demais meios individuais de acesso são pessoais e não deverão ser compartilhados.

Cada pessoa é responsável pela guarda e utilização dos meios de acesso sob sua responsabilidade.

Perda, extravio, comprometimento ou suspeita de utilização indevida deverão ser comunicados imediatamente.

## 5. Acesso físico

O acesso às unidades e ambientes físicos da BrisaLuz deverá respeitar as autorizações estabelecidas para cada local.

Áreas sujeitas a maior controle operacional poderão possuir mecanismos adicionais de segurança e restrição.

O ingresso em determinada unidade não representa autorização irrestrita para ingresso em todas as suas áreas.

Portas, portões, grades, barreiras e demais estruturas destinadas ao controle de acesso deverão permanecer nas condições de segurança estabelecidas para cada ambiente.

## 6. Catracas, fechaduras e controles eletrônicos

Catracas, fechaduras eletrônicas, leitores, cartões, códigos, aplicativos ou dispositivos equivalentes deverão ser utilizados de acordo com sua finalidade e, quando individualizados, exclusivamente pela pessoa autorizada.

Não deverá ser facilitado o ingresso de pessoa não identificada ou não autorizada mediante aproveitamento da liberação concedida a terceiro.

Falhas, violações, danos ou funcionamento irregular dos mecanismos de controle deverão ser comunicados.

A indisponibilidade ou defeito de mecanismo de controle não constitui autorização para ingresso irrestrito no ambiente protegido.

## 7. Chaves

Chaves de unidades, salas, armários, depósitos ou demais ambientes controlados deverão permanecer sob responsabilidade das pessoas autorizadas.

Quando houver sistema de controle de chaves, sua retirada, transferência e devolução deverão ser registradas.

É vedada a realização de cópias sem autorização.

A perda, extravio ou suspeita de reprodução não autorizada deverá ser comunicada imediatamente.

Encerrada a necessidade de acesso, a chave deverá ser devolvida ou destinada conforme determinação institucional.

## 8. Sistema Institucional de Registro

A BrisaLuz AFA mantém sistema eletrônico institucional para registro individual de presença, acesso e atividade, disponível em:

<https://brisaluz.atipicaluz.org/wpchef-attendance-clock/>

O registro no sistema é **obrigatório para todas as pessoas submetidas ao controle institucional de presença, acesso ou atividade**, independentemente de cargo, função ou natureza do vínculo com a BrisaLuz AFA.

O registro é pessoal e de responsabilidade de quem o realiza, devendo corresponder fielmente à presença ou atividade efetivamente ocorrida.

É vedado: **I** - realizar registro em nome de terceiro; **II** - solicitar que terceiro realize registro em seu nome; **III** - permitir a utilização de credenciais pessoais por terceiro; **IV** - inserir informação deliberadamente incompatível com a presença ou atividade efetivamente ocorrida.

O sistema constitui mecanismo formal de registro e rastreabilidade institucional.

## 9. Registro de acesso físico

O ingresso em unidade ou ambiente físico sujeito ao controle institucional deverá ser acompanhado do correspondente registro no sistema.

A saída deverá igualmente ser registrada, permitindo identificar o período de presença.

Quando houver interrupção temporária da presença ou da atividade, deverão ser utilizados os recursos de interrupção e retorno disponibilizados pelo sistema, quando aplicáveis.

O registro no sistema não substitui os demais mecanismos de segurança e controle existentes no ambiente.

## 10. Registro de acesso virtual

O início de atividade em ambiente virtual sujeito ao controle institucional deverá ser acompanhado do correspondente registro no sistema.

Interrupções deverão ser registradas quando representarem efetiva suspensão da atividade.

O retorno e o encerramento deverão igualmente ser registrados.

Os registros deverão representar fielmente os períodos de atividade institucional.

## 11. Acesso virtual e credenciais

O acesso aos ambientes virtuais da BrisaLuz compreende, entre outros, **WhatsApp institucional, sistemas de atendimento, contas de e-mail, plataformas administrativas, sistemas de gestão, armazenamento de arquivos, bancos de dados, redes sociais institucionais e demais serviços digitais utilizados pela Associação.**

O acesso deverá ocorrer, sempre que tecnicamente possível, mediante identificação individual.

Cada pessoa deverá utilizar somente contas, perfis, funcionalidades e permissões compatíveis com sua autorização.

O acesso ao **WhatsApp institucional**, ainda que realizado por dispositivo pessoal, computador ou equipamento autorizado, permanece sujeito às regras institucionais de identificação, segurança, sigilo e rastreabilidade.

Senhas, códigos, tokens, códigos de verificação, QR Codes de vinculação de dispositivos e demais credenciais não deverão ser compartilhados com pessoas não autorizadas.

A vinculação de novos dispositivos às contas institucionais somente poderá ocorrer mediante autorização.

Sessões abertas deverão ser encerradas ou protegidas quando houver possibilidade de utilização por terceiro.

É vedado acessar conversas, informações, arquivos, funcionalidades ou recursos estranhos à finalidade que justificou o acesso.

## 12. Mecanismos complementares de segurança e fiscalização

O registro realizado no Sistema Institucional de Registro é de responsabilidade pessoal e constitui um dos mecanismos de controle e rastreabilidade adotados pela BrisaLuz AFA.

Sua utilização não impede, limita ou substitui outros mecanismos de segurança, fiscalização e registro.

**I** - câmeras de segurança; **II** - sensores; **III** - catracas; **IV** - fechaduras e controles eletrônicos; **V** - alarmes; **VI** - controle de chaves; **VII** - registros de abertura e fechamento; **VIII** - registros de acesso e atividade em sistemas, equipamentos, WhatsApp institucional e demais plataformas digitais; **IX** - registros operacionais e documentais; **X** - outros mecanismos legítimos de segurança e rastreabilidade.

Os diferentes mecanismos poderão ser relacionados entre si para reconstrução e verificação dos acessos e atividades ocorridos.

## 13. Associados, visitantes e terceiros

Associados, visitantes, fornecedores, prestadores eventuais e demais terceiros que necessitem ingressar em ambiente sujeito a controle deverão observar as regras aplicáveis ao respectivo local.

Quando exigida autorização, o acesso ficará limitado à finalidade, área e período que o justificaram.

Quando necessário, a pessoa deverá permanecer acompanhada por pessoa autorizada.

Encerrada a finalidade que justificou o acesso, deverá ser encerrada a respectiva autorização.

## 14. Áreas de acesso restrito

Determinadas áreas poderão possuir acesso restrito em razão de sua natureza, dos materiais nelas mantidos, das atividades desenvolvidas ou da necessidade de preservação da segurança e rastreabilidade.

O acesso ficará limitado às pessoas autorizadas e aos limites da autorização concedida.

A autorização geral de ingresso em determinada unidade não afasta as restrições específicas existentes em seu interior.

## 15. Alteração e encerramento de acessos

Alteradas as circunstâncias que justificaram determinada autorização, deverá ser avaliada sua manutenção, ampliação, redução ou encerramento.

Cessada a necessidade de acesso, deverão ser devolvidos, cancelados ou desabilitados, conforme o caso, chaves, cartões, códigos, usuários, permissões e demais meios de acesso.

## 16. Divergências e irregularidades

Os registros realizados no sistema institucional poderão ser confrontados com os demais mecanismos de segurança, fiscalização e rastreabilidade mantidos pela BrisaLuz AFA.

Erros ou omissões identificados deverão ser comunicados para regularização.

Divergências relevantes ou reiteradas poderão ser submetidas à verificação institucional.

Registros deliberadamente falsos, utilização indevida de credenciais, manipulação de controles ou qualquer conduta destinada a impedir ou comprometer a identificação e a rastreabilidade constituem não conformidade institucional.

## 17. Incidentes de segurança

Deverão ser comunicados tão logo identificados: **I** - perda ou extravio de chave, cartão ou credencial; **II** - acesso ou tentativa de acesso não autorizado; **III** - compartilhamento ou utilização indevida de credencial; **IV** - violação, dano ou defeito em mecanismo de segurança; **V** - presença não identificada em ambiente controlado; **VI** - acesso virtual incompatível com a autorização existente; **VII** - divergência relevante nos registros; **VIII** - qualquer situação capaz de comprometer a segurança, identificação, controle ou rastreabilidade.

## 18. Rastreabilidade dos acessos

Os registros de presença, acesso e atividade integram os mecanismos institucionais de segurança e rastreabilidade da BrisaLuz AFA.

Os mecanismos adotados deverão permitir, conforme sua natureza, identificar **quem acessou, onde acessou, quando ocorreu o acesso e o período correspondente**.

Os registros poderão ser relacionados aos demais registros operacionais e institucionais para fins de segurança, rastreabilidade, auditoria, apuração de ocorrências e prevenção ao desvio de finalidade.

## 19. Disposição operacional final

Na dúvida quanto à existência ou extensão de autorização para acessar determinada unidade, área, sistema, informação ou recurso, a autorização não será presumida.

A pessoa deverá obter orientação ou autorização do responsável correspondente antes de realizar o acesso.

As situações não previstas neste Manual serão submetidas ao **MN005.v1 - Segurança e Controle de Acesso** e às demais normas institucionais aplicáveis.