WHITEPAPER

CONTROLE DE ACESSO EM SUBESTAÇÕES: PESSOAS, VEÍCULOS E INTEGRAÇÃO

Entenda como projetar controle de acesso em subestações: zonas, pessoas, veículos, visitantes, credenciais, integração, cibersegurança e testes.

A3A® Engenharia de Sistemas

SUMÁRIO

O **controle de acesso em subestações** precisa relacionar pessoas, veículos, áreas, horários, autorizações e procedimentos em uma instalação com ativos críticos, risco elétrico, equipes próprias, empresas contratadas e períodos sem presença permanente.

Uma credencial válida para entrar no empreendimento não significa que a pessoa esteja autorizada a acessar o pátio elétrico, uma sala de proteção ou executar atividades em uma zona controlada. O sistema eletrônico aplica regras de passagem e registra eventos, mas não substitui qualificação, capacitação, autorização formal, análise de risco nem procedimentos de trabalho.

O projeto deve começar por cinco perguntas: quem pode acessar, onde, quando, em quais condições e com qual registro. Essas respostas são transformadas em zonas, perfis, credenciais, dispositivos, integrações e testes verificáveis.

1. O QUE MUDA NO CONTROLE DE ACESSO DE UMA SUBESTAÇÃO

Uma subestação reúne áreas com níveis distintos de criticidade. Portão externo, casa de controle, salas técnicas, banco de baterias, depósitos e pátio elétrico não devem ser tratados como uma única permissão.

Também existem motivos diferentes para ingresso. Operadores, equipes de manutenção, empresas contratadas, visitantes e atendimento emergencial precisam de regras próprias, com validade, horários, responsáveis e limites de circulação.

A NR-10 diferencia qualificação, habilitação, capacitação e autorização de trabalhadores que interagem com instalações elétricas. O controle de acesso pode ajudar a aplicar a abrangência de uma autorização e impedir passagens incompatíveis, mas a liberação física não concede autorização para executar serviços elétricos.

2. ZONAS, PERFIS E MATRIZ DE ACESSO

O projeto deve dividir a instalação em zonas coerentes com os riscos e com a operação. Essa setorização evita que uma credencial permita acesso indiscriminado a áreas que exigem responsabilidades ou procedimentos diferentes.

Uma arquitetura pode distinguir perímetro, ponto de identificação, casa de controle, salas técnicas, depósitos, áreas administrativas e pátio elétrico. A quantidade de zonas depende do arranjo, do regime operacional e dos critérios do proprietário.

A matriz de acesso conecta pessoas e áreas. Ela deve indicar perfil, zona, horário, condição de liberação, necessidade de acompanhamento, prazo de validade e tratamento

de tentativas indevidas.

PerfilÁreas típicasCondições possíveisOperaçãocasa de controle e áreas operacionais definidasvínculo ativo, autorização formal e escala aplicávelManutençãoáreas relacionadas ao serviçoordem de trabalho, janela autorizada e requisitos de segurançaEmpresa contratadazonas delimitadas pelo escopocredencial temporária, responsável interno e vencimentoVisitanterota e áreas previamente definidascadastro, identificação e acompanhamentoEmergênciaáreas previstas no plano de respostaprocedimento, registro e supervisão

A matriz deve prever exceções. Uma pessoa pode ter acesso regular à casa de controle e necessitar de aprovação adicional para o pátio. Uma credencial temporária deve expirar automaticamente ao final da atividade.

O Guia Completo sobre Controle de Acesso aprofunda os princípios de quem, onde e quando. Em subestações, eles precisam ser associados à segurança elétrica e aos procedimentos da instalação.

3. FUNCIONÁRIOS, EMPRESAS CONTRATADAS E VISITANTES

O ciclo de vida da identidade é tão importante quanto o leitor instalado na porta. O sistema precisa prever cadastro, aprovação, emissão, alteração, suspensão, vencimento e revogação das credenciais.

Para trabalhadores próprios, os perfis devem refletir função, local de atuação e abrangência da autorização. Mudanças de função, afastamentos, vencimentos ou transferências precisam gerar revisão das permissões.

Empresas contratadas exigem controle adicional porque o vínculo é temporário e relacionado a um escopo. O acesso pode depender de contrato ativo, documentação aprovada, responsável interno, ordem de trabalho e período autorizado. A credencial deve perder validade quando uma condição essencial deixa de ser atendida.

Visitantes devem passar por pré-cadastro, confirmação do responsável, identificação, emissão de credencial temporária e definição de rota. O sistema precisa registrar entrada, áreas liberadas e saída, sem coletar dados além do necessário.

Em instalações desassistidas, interfonia IP e vídeo podem apoiar a identificação remota. A liberação deve seguir procedimento documentado, registrando quem solicitou, quem autorizou e quais condições foram verificadas.

4. CONTROLE DE ACESSO DE VEÍCULOS

Portões de veículos concentram riscos patrimoniais e operacionais. Além de autorizar a entrada, o sistema deve relacionar veículo, condutor, finalidade e vínculo com pessoas ou serviços autorizados.

Tags UHF permitem identificação sem contato. O reconhecimento automático de placas pode complementar a decisão e fornecer evidência visual, mas não deve ser tratado isoladamente como prova da identidade do condutor. Em instalações críticas, pode ser adequado combinar credencial veicular, credencial pessoal e imagem contextual.

A engenharia do acesso envolve laços indutivos, sensores de presença, cancelas, portões, semáforos, intertravamentos e dispositivos de segurança. A lógica deve evitar fechamento sobre veículos, abertura simultânea indevida, entrada por acompanhamento e permanência do portão aberto além do necessário.

Veículos leves, caminhões, equipes de manutenção e atendimento emergencial podem exigir regras diferentes. O projeto deve considerar área de espera, manobra, visibilidade, comunicação e comportamento durante falhas de energia ou comunicação.

5. CREDENCIAIS E MÉTODOS DE AUTENTICAÇÃO

Não existe uma credencial universalmente superior. A escolha depende do risco, do ambiente, da frequência de uso, dos equipamentos de proteção, da privacidade e da capacidade de administrar o ciclo de vida.

Smart cards podem oferecer recursos criptográficos e são adequados para uso recorrente. Credenciais móveis simplificam emissão e revogação, mas dependem da política de dispositivos. PINs podem ser compartilhados. Códigos QR funcionam para visitantes com validade curta. Biometria vincula o acesso a uma característica da pessoa, porém exige avaliação de desempenho e proteção dos dados.

MétodoAplicação possívelCuidados principaisSmart cardequipes próprias e terceiros recorrentestecnologia, chaves, emissão e revogaçãoCredencial móvelusuários corporativossegurança do dispositivo e recuperaçãoBiometriaconfirmação adicional em pontos críticosambiente, LGPD e contingênciaPINsegundo fatorcompartilhamento e política de trocaQR temporáriovisitantesvalidade curta e uso controladoTag UHF ou LPRveículosassociação ao condutor e leitura indevida

A autenticação multifator pode ser adequada para áreas sensíveis. A complexidade deve ser proporcional ao risco e não pode criar atalhos que levem as equipes a contornar o

sistema.

O projeto também deve definir contingências para falha de leitor, biometria, servidor ou comunicação, mantendo segurança e rastreabilidade.

6. DISPOSITIVOS DE CAMPO E COMPORTAMENTO DAS PORTAS

Leitor, controladora, fechadura, contato de porta, botão de saída, sensor e fonte precisam funcionar como um conjunto.

A controladora deve manter decisões e eventos locais quando a comunicação com o servidor for interrompida. O contato de porta diferencia uma passagem autorizada de uma porta forçada ou mantida aberta.

Fechaduras eletromagnéticas, eletromecânicas, contrafechos, torniquetes, cancelas e portões possuem comportamentos diferentes durante falta de energia. A escolha entre liberação e manutenção do travamento deve considerar evacuação, proteção patrimonial, emergência e uso do ambiente. Não existe uma regra única para todas as portas.

Em áreas externas, leitores e atuadores precisam ser adequados a chuva, poeira, temperatura, impacto, corrosão e exposição solar. Em subestações, também devem ser avaliados compatibilidade eletromagnética, rotas, equipotencialização e proteção contra surtos.

7. ARQUITETURA, AUTONOMIA LOCAL E ALIMENTAÇÃO

O sistema pode ser centralizado, distribuído ou híbrido. Em subestações remotas, a autonomia local é essencial: a perda da WAN ou do servidor corporativo não deve eliminar as regras básicas de acesso nem os registros.

Controladoras locais podem manter credenciais, horários e estados de portas. Após a recuperação da comunicação, os eventos devem ser sincronizados sem perda de sequência ou duplicidade.

A rede precisa ser segmentada conforme a criticidade. Dispositivos de segurança física não devem ser conectados indiscriminadamente às redes de automação ou supervisão. Integrações precisam usar interfaces e regras definidas.

A alimentação deve abranger leitores, controladoras, fechaduras, switches, servidores e enlaces. UPS, fontes supervisionadas e baterias devem considerar autonomia, consumo e cenários de falha. Manter apenas o software ativo não preserva a função se as portas ou controladoras estiverem indisponíveis.

Sincronismo de tempo, backups e inventário também são essenciais para correlacionar eventos de acesso, imagens e alarmes.

8. INTEGRAÇÃO COM CFTV, PERÍMETRO E INTERFONIA

Uma tentativa negada pode apresentar a câmera correspondente; uma porta forçada pode iniciar gravação prioritária; um visitante pode ser associado ao responsável interno; e um evento perimetral pode orientar a supervisão de rotas específicas.

O CFTV patrimonial em subestações fornece a camada visual. A Proteção perimetral em subestações detecta aproximação e cruzamento das divisas. O controle de acesso administra passagens autorizadas. As disciplinas devem compartilhar eventos, preservando critérios próprios de desempenho.

Interfonia IP permite comunicação antes da liberação. Em instalações remotas, o operador pode visualizar a cena, confirmar o cadastro e registrar a decisão. O desenho precisa prever indisponibilidade do enlace e contingência local.

A integração com o monitoramento patrimonial deve produzir uma sequência rastreável: evento, apresentação da cena, decisão, liberação ou bloqueio, registro e encerramento.

9. CIBERSEGURANÇA, OSDP E MODERNIZAÇÃO

Sistemas modernos possuem dispositivos conectados, servidores, bancos de dados, credenciais e integrações. Por isso, fazem parte da superfície de ataque da organização.

A arquitetura deve incluir segmentação, autenticação administrativa, menor privilégio, registros, backups, atualização controlada, certificados e gestão de vulnerabilidades. O acesso remoto deve ser limitado e monitorado.

Interfaces legadas como Wiegand oferecem pouca supervisão. O OSDP foi desenvolvido para melhorar interoperabilidade, comunicação bidirecional e supervisão; quando implementado com canal seguro, permite criptografia entre dispositivos compatíveis. A adoção depende do suporte real dos equipamentos e de testes de interoperabilidade.

A modernização pode preservar componentes tecnicamente adequados e substituir gradualmente credenciais frágeis, controladoras sem suporte e integrações limitantes. Para operações com várias unidades, os artigos sobre Arquitetura de Controle de Acesso Corporativo e Controle de Acesso Enterprise complementam o tema.

10. BIOMETRIA, DADOS PESSOAIS E PRIVACIDADE

A biometria pode aumentar a confiança de que a credencial está sendo usada pela pessoa cadastrada, mas não deve ser escolhida apenas pela percepção de modernidade. Poeira, umidade, iluminação, luvas, capacetes e máscaras afetam diferentes tecnologias.

O projeto precisa testar aceitação e rejeição no ambiente real e prever alternativa para pessoas que não possam utilizar a modalidade ou para situações de falha.

Dados biométricos vinculados a uma pessoa são dados pessoais sensíveis segundo a LGPD. A organização deve definir finalidade, necessidade, segurança, retenção, compartilhamento e descarte. O cadastro precisa verificar a identidade e a revogação deve ocorrer quando o vínculo ou a autorização terminar.

11. PROJETO, COMISSIONAMENTO E MANUTENÇÃO

O projeto deve transformar políticas e riscos em requisitos verificáveis, incluindo levantamento, matriz de acesso, arquitetura, infraestrutura, autonomia, integrações, cibersegurança e critérios de aceite.

O comissionamento precisa testar a cadeia completa:

1. acesso permitido e negado por perfil e zona; 2. credencial vencida, suspensa ou fora do horário; 3. porta forçada, mantida aberta e tentativa de acompanhamento; 4. ingresso e saída de visitantes, terceiros e veículos; 5. perda de servidor, WAN, controladora, leitor e fonte; 6. integração com vídeo, interfonia e alarmes; 7. recuperação da comunicação e sincronização dos eventos.

A documentação final deve registrar portas, controladoras, leitores, circuitos, fontes, zonas, perfis, regras, versões e backups. Mudanças posteriores precisam seguir gestão de configuração.

A manutenção inclui inspeção física, testes, revisão de baterias e fontes, verificação de eventos, atualização controlada, auditoria de usuários e revisão periódica das permissões.

Erros recorrentes incluem confundir passagem física com autorização para trabalho elétrico, usar um perfil único para toda a instalação, manter credenciais temporárias sem vencimento, depender totalmente da WAN e instalar leitores externos inadequados ao ambiente.

12. CONCLUSÃO

O controle de acesso em subestações deve conectar identidade, autorização, área, horário e condição operacional. Seu objetivo não é apenas permitir ou negar passagens, mas aplicar políticas de forma rastreável e compatível com os riscos da instalação.

Uma solução consistente combina matriz de acesso, dispositivos de campo, autonomia local, energia auxiliar, integração, cibersegurança e procedimentos. Essas camadas contribuem para a segurança patrimonial e para a governança do acesso sem substituir as responsabilidades formais de segurança elétrica.

Cadastro, revisão de perfis, revogação, manutenção, atualizações e testes periódicos fazem parte da solução tanto quanto leitores e controladoras.

[1] ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR IEC 60839-11-1 — Sistemas eletrônicos de controle de acesso — Requisitos de sistema e componentes. Consultar edição vigente no Catálogo ABNT.

[2] ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR IEC 60839-11-2 — Sistemas eletrônicos de controle de acesso — Diretrizes de aplicação. Consultar edição vigente no Catálogo ABNT.

[3] BRASIL. Ministério do Trabalho e Emprego. NR-10 — Segurança em Instalações e Serviços em Eletricidade. Consultar texto oficial vigente.

[4] BRASIL. Lei nº 13.709, de 14 de agosto de 2018 — Lei Geral de Proteção de Dados Pessoais.

[5] SECURITY INDUSTRY ASSOCIATION. Open Supervised Device Protocol — OSDP.

Qual é a diferença entre acesso físico e autorização conforme a NR-10? O acesso físico permite ou bloqueia a passagem. A autorização para intervir em instalações elétricas depende dos requisitos formais de qualificação, capacitação, habilitação, treinamento e anuência da empresa.**Quais áreas de uma subestação devem ter controle de acesso?** A definição depende do arranjo e do risco, podendo incluir perímetro, casa de controle, salas técnicas, bancos de baterias, depósitos e pátio elétrico.**Como controlar empresas contratadas?** O acesso pode ser condicionado a contrato ativo, documentação aprovada, responsável interno, ordem de serviço e credencial temporária com vencimento automático.**Qual é a melhor credencial para uma subestação?** Não existe uma opção única. Smart cards, credenciais móveis, biometria, QR temporário e tags veiculares devem ser avaliados conforme risco, ambiente e contingência.**Biometria pode ser usada com**

equipamentos de proteção? Depende da modalidade e do ambiente. Luvas, máscaras, capacetes, iluminação, poeira e umidade podem afetar a leitura.**Como controlar veículos autorizados?** É possível combinar tag veicular, reconhecimento de placa, credencial do condutor, sensores, cancelas e imagem contextual.**O sistema deve funcionar sem o servidor central?** Em instalações remotas, controladoras locais podem manter regras e eventos durante a perda da WAN, sincronizando os registros após a recuperação.**O que é OSDP?** É um protocolo de comunicação para controle de acesso com interoperabilidade, supervisão e comunicação bidirecional. O canal seguro permite criptografia quando suportado.**Como integrar controle de acesso e CFTV?** Eventos como acesso negado ou porta forçada podem apresentar câmeras relacionadas, iniciar gravação prioritária e registrar a decisão do operador.**O que deve ser testado no comissionamento?** Perfis, horários, credenciais, portas, veículos, visitantes, integrações, autonomia, perda de comunicação, recuperação e documentação final.

Soluções

Serviços de engenharia

Materiais técnicos complementares

Conteúdos correlatos

Sobre a A3A Engenharia de Sistemas

Com 30 anos de história, a A3A Engenharia de Sistemas se consolidou como referência em serviços de Engenharia, oferecendo soluções integradas de Telecomunicações, Segurança Eletrônica, Segurança Digital e Instalações Elétricas.

A empresa atua em todas as etapas do ciclo de Engenharia, desde a elaboração de projetos e consultoria técnica até a implantação, manutenção e retrofit de sistemas, sempre em conformidade com as normas técnicas e melhores práticas do setor.

A3A® Engenharia de Sistemas