WHITEPAPER

CIBERSEGURANÇA EM SISTEMAS DE CFTV: ARQUITETURA, HARDENING E GESTÃO DE RISCOS

A3A® Engenharia de Sistemas

SUMÁRIO

1. SUMÁRIO EXECUTIVO

Um sistema de CFTV IP é uma infraestrutura distribuída de tecnologia da informação formada por câmeras, encoders, switches, servidores, VMS, bancos de dados, storage, estações de operação, aplicativos móveis, integrações e serviços remotos. Cada componente amplia a capacidade de monitoramento, mas também adiciona identidades, interfaces, protocolos, softwares e dependências que precisam ser protegidos.

A cibersegurança do CFTV não pode ser reduzida à troca da senha padrão. O sistema precisa preservar a **confidencialidade** das imagens e configurações, a **integridade** das gravações e registros, a **disponibilidade** da operação e a **rastreabilidade** das ações administrativas e operacionais. Esses objetivos devem orientar o projeto, a implantação, o aceite, a manutenção e o descarte dos ativos.

Este whitepaper apresenta um método de engenharia para estruturar a cibersegurança em sistemas de videomonitoramento. O método combina requisitos setoriais da ABNT NBR IEC 62676, gestão de riscos da família ISO/IEC 27000, segmentação por zonas, práticas NIST e recomendações de hardening de fabricantes de câmeras e VMS.

ObjetivoRisco típicoResultado esperadoConfidencialidadeAcesso indevido a imagens, áudio, mapas ou cadastrosIdentidades individuais, menor privilégio, criptografia e controle de exportaçãoIntegridadeAlteração de configuração, tempo, gravações ou registrosControle de mudanças, autenticação dos dados, logs e preservação de evidênciasDisponibilidadePerda de vídeo, gravação, storage, rede ou VMSMonitoramento, redundância compatível com o risco e recuperação documentadaRastreabilidadeUso de contas compartilhadas ou ações sem registroAuditoria de acessos, mudanças, buscas, exportações e falhasPrivacidadeTratamento excessivo ou retenção sem justificativaFinalidade, acesso controlado, retenção definida e governança das imagens

2. SUPERFÍCIE DE ATAQUE DE UM SISTEMA DE CFTV IP

A superfície de ataque inclui todos os pontos pelos quais uma pessoa, dispositivo ou software pode interagir com o sistema. Câmeras possuem serviços web, protocolos de streaming, APIs, mecanismos de descoberta, cartões de memória e, em alguns casos, aplicações embarcadas. O VMS depende de sistemas operacionais, bancos de dados, certificados, serviços de gravação, clientes, diretórios de usuários e integrações.

O risco aumenta quando dispositivos permanecem com firmware sem suporte, quando a rede é plana, quando portas são liberadas sem necessidade, quando o acesso remoto contorna os controles corporativos ou quando fornecedores utilizam contas permanentes e compartilhadas. A exposição não precisa ser pública para ser relevante: um

equipamento comprometido na rede corporativa pode alcançar o CFTV quando não existe segmentação adequada.

ComponenteExposições comunsControles prioritáriosCâmeras e encodersCredenciais fracas, serviços desnecessários, firmware vulnerável e acesso físicoHardening, certificados, 802.1X, atualização e proteção do dispositivoRedeVLAN única, fluxos não controlados, descoberta ampla e acesso lateralZonas, ACLs, firewall, monitoramento e documentação dos fluxosVMS e servidoresServiços expostos, privilégios excessivos, sistema operacional desatualizadoHardening do servidor, menor privilégio, patches, backup e logsStorageExclusão, indisponibilidade, acesso direto ou retenção inadequadaPermissões, redundância, monitoramento, proteção e testes de recuperaçãoClientes e operadoresContas compartilhadas, exportações sem controle e estações comprometidasPerfis, MFA quando aplicável, auditoria e endurecimento das estaçõesIntegraçõesAPIs sem restrição, segredos expostos e confiança excessiva entre sistemasContas técnicas dedicadas, escopo mínimo, TLS e monitoramentoAcesso remotoPort forwarding, VPN sem governança ou suporte permanente do fornecedorGateway controlado, MFA, aprovação, tempo limitado e registro da sessão

3. BASE NORMATIVA E TÉCNICA

A ABNT NBR IEC 62676-1-1 trata a segurança do sistema de videomonitoramento a partir da integridade do sistema e da integridade dos dados. Entre os temas relevantes estão controle de acesso físico e lógico, detecção de falhas, proteção contra violação, identificação da fonte, carimbo de tempo, autenticação, proteção das gravações, registros de atividades, backup, exportação e monitoramento das interconexões.

A ABNT NBR ISO/IEC 27001 fornece a estrutura de gestão: contexto, responsabilidades, avaliação e tratamento de riscos, controles documentados, auditoria e melhoria contínua. A ABNT NBR ISO/IEC 27032 complementa essa abordagem para sistemas conectados à internet, incluindo gestão de vulnerabilidades, ativos, rede, incidentes, mudanças, criptografia e endpoints.

Em instalações industriais, subestações e ambientes nos quais o CFTV interage com automação, SCADA ou redes operacionais, os conceitos da ABNT IEC/TS 62443-1-1 ajudam a definir defesa em profundidade, zonas, conduítes e níveis de segurança. Essa aplicação deve ser contextualizada: a IEC 62443 não é uma norma universal de CFTV, mas uma referência importante quando o sistema influencia ou compartilha infraestrutura com ambientes de tecnologia operacional.

O método também utiliza o NIST CSWP 28 para segmentação, o guia de hardening do AXIS OS para dispositivos de borda e o guia de hardening do Milestone XProtect para VMS, servidores, clientes e rede. As edições vigentes das normas devem ser verificadas no Catálogo ABNT.

Cibersegurança precisa fazer parte do projeto do CFTV.

Quando segmentação, certificados, perfis, logs, atualização e recuperação são definidos somente após a implantação, surgem dependências difíceis de corrigir e indisponibilidades durante a adequação.

Conhecer o Projeto de Sistema Integrado de Segurança Eletrônica

4. MODELO DE CIBERSEGURANÇA PARA CFTV

O modelo proposto está organizado em doze domínios. Eles não são etapas isoladas; formam um ciclo contínuo de projeto, operação, avaliação e melhoria.

4.1. 1. GOVERNANÇA, ESCOPO E RESPONSABILIDADES

O primeiro passo é definir quem responde pelo sistema, pela rede, pelos servidores, pelas câmeras, pelos usuários, pelas imagens, pelas atualizações e pelo atendimento a incidentes. Segurança patrimonial, TI, infraestrutura, jurídico, privacidade, fornecedores e operação possuem responsabilidades distintas e precisam compartilhar critérios de decisão.

O escopo deve registrar unidades, ambientes, tecnologias, integrações, serviços em nuvem, acessos remotos e dados tratados. Sem esse limite, ativos ficam fora do inventário e vulnerabilidades deixam de ter proprietário.

4.2. 2. INVENTÁRIO E CLASSIFICAÇÃO DOS ATIVOS

O inventário relaciona equipamento, modelo, número de série, endereço, localização, função, versão de firmware, suporte, credenciais administradas, certificados, VLAN, portas, integrações e responsável. Também deve incluir VMS, plugins, drivers, servidores, sistemas operacionais, bancos de dados, storage, clientes e aplicativos móveis.

A classificação considera criticidade operacional, sensibilidade das imagens, exposição, impacto da indisponibilidade e dependência de outros sistemas. Uma câmera de perímetro em instalação crítica não deve receber o mesmo tratamento de um dispositivo auxiliar em área administrativa.

4.3. 3. SEGMENTAÇÃO POR ZONAS E FLUXOS PERMITIDOS

A rede deve separar ativos com funções e requisitos diferentes. Uma arquitetura típica pode possuir zona de câmeras, zona de servidores e gravação, zona de operação, zona administrativa, zona de integrações e um ponto controlado para acesso remoto. As fronteiras são protegidas por ACLs ou firewalls, e os fluxos são liberados conforme necessidade documentada.

ZonaAtivosComunicações esperadasBorda de vídeoCâmeras, encoders, intercoms e dispositivos IPVMS, NTP, DNS, gestão e serviços estritamente necessáriosVMS e gravaçãoManagement, recording, banco e storageBorda, clientes autorizados, diretório, backup e monitoramentoOperaçãoEstações e videowallServiços do VMS e integrações autorizadasAdministraçãoEstações técnicas e ferramentas de gestãoAcesso privilegiado controlado aos componentesIntegraçãoPSIM, controle de acesso, analíticos e APIsInterfaces específicas, contas técnicas e portas definidasAcesso remotoVPN, bastion ou gatewaySessões autenticadas, aprovadas, registradas e limitadas

A segmentação não termina na criação de VLANs. É necessário controlar o tráfego entre elas, remover caminhos alternativos e verificar periodicamente se os fluxos observados correspondem à arquitetura aprovada.

4.4. 4. IDENTIDADES, AUTENTICAÇÃO E MENOR PRIVILÉGIO

Usuários administrativos, operadores, auditores, manutenção e integrações precisam de contas distintas. Perfis devem limitar visualização, reprodução, exportação, configuração, manutenção e acesso a câmeras específicas. Contas genéricas dificultam responsabilização e devem ser eliminadas sempre que a plataforma permitir identidade individual.

Senhas devem seguir política corporativa, e autenticação multifator deve ser aplicada a acessos remotos e administrativos quando suportada. Contas técnicas precisam de finalidade, proprietário, segredo protegido, rotação e escopo mínimo.

4.5. 5. HARDENING DAS CÂMERAS E DISPOSITIVOS DE BORDA

O hardening reduz a superfície de ataque por configuração. O guia do AXIS OS recomenda autenticação obrigatória, HTTPS, proteção contra replay em interfaces ONVIF, mecanismos contra força bruta, logs de auditoria, desativação de protocolos não utilizados, 802.1X com certificados e proteção adicional do enlace quando suportada.

Na prática, a linha de base deve definir serviços permitidos, protocolos de descoberta, política HTTP/HTTPS, certificados, NTP, DNS, syslog, SNMP, contas, aplicações embarcadas, armazenamento local, áudio, entradas e saídas. Recursos não utilizados devem permanecer desabilitados.

4.6. 6. HARDENING DO VMS, SERVIDORES, CLIENTES E STORAGE

O VMS depende do sistema operacional e de serviços associados. O hardening inclui instalação mínima, atualização controlada, firewall local, proteção antimalware compatível, restrição de administração, contas de serviço com menor privilégio, proteção do banco de dados, backup das configurações e desativação de componentes desnecessários.

Estações de operação não devem ser tratadas como computadores comuns de uso irrestrito. Navegação, e-mail, instalação de software e mídias removíveis ampliam o risco. O storage precisa de permissões restritas, monitoramento de capacidade, proteção contra exclusão indevida e testes de recuperação.

4.7. 7. COMUNICAÇÃO SEGURA E CRIPTOGRAFIA

HTTPS e TLS protegem interfaces e APIs; SRTP ou RTSPS podem proteger fluxos de mídia quando suportados pela arquitetura; 802.1X autentica dispositivos na porta de rede; e MACsec pode proteger enlaces Ethernet específicos. A escolha deve considerar compatibilidade, desempenho, gestão de certificados e impacto operacional.

Criptografar apenas a interface web não protege necessariamente o vídeo, os metadados ou os dados exportados. O projeto deve mapear cada fluxo, identificar onde existe informação sensível e definir o controle aplicável. Certificados precisam de inventário, autoridade confiável, prazo de validade e processo de renovação.

4.8. 8. ACESSO REMOTO E SUPORTE DE FORNECEDORES

Port forwarding direto para câmeras, gravadores ou VMS deve ser evitado. O acesso remoto deve passar por solução corporativa controlada, com identidade individual, MFA, autorização, prazo, registro e revogação. Em ambientes críticos, pode ser exigida estação intermediária, gravação da sessão e aprovação para cada intervenção.

A relação com fornecedores precisa definir quem pode acessar, em quais condições, como vulnerabilidades serão comunicadas, por quanto tempo haverá suporte e como credenciais e dados serão devolvidos ou eliminados ao término do contrato.

4.9. 9. LOGS, AUDITORIA E MONITORAMENTO

O sistema deve registrar autenticações, acessos negados, mudanças de configuração, reinicializações, falhas, perda e recuperação de vídeo, buscas, reproduções, exportações e ações sobre alarmes. A sincronização de tempo é essencial para correlacionar eventos entre câmeras, VMS, controle de acesso, firewall e diretório.

Logs locais podem ser perdidos com a falha ou comprometimento do dispositivo. Quando o risco justificar, devem ser enviados a uma plataforma central, protegidos contra alteração e retidos por período definido. Alertas precisam distinguir falha operacional, evento de segurança e indisponibilidade de infraestrutura.

4.10. 10. VULNERABILIDADES, FIRMWARE E GESTÃO DE MUDANÇAS

Atualização não deve ocorrer de forma improvisada, mas também não pode ser adiada indefinidamente. O processo inclui monitorar avisos e CVEs, verificar aplicabilidade, avaliar criticidade, testar compatibilidade, criar backup, programar janela, atualizar, validar funções e registrar o resultado.

Mudanças em firmware, drivers, VMS, certificados, regras de rede ou integrações devem possuir solicitação, análise de impacto, plano de retorno e evidência de teste. A linha de base de configuração permite identificar desvios e reconstruir o sistema.

4.11. 11. INTEGRIDADE DAS GRAVAÇÕES, EXPORTAÇÃO E PRIVACIDADE

A ABNT NBR IEC 62676 destaca identificação da fonte, data e hora, proteção contra manipulação, registros e exportação preservando a gravação original. Uma evidência precisa manter contexto, metadados, sequência temporal e mecanismo de reprodução. Alterações realizadas para visualização ou melhoria não devem substituir o original.

Do ponto de vista da LGPD, imagens associadas a pessoas identificadas ou identificáveis exigem finalidade, base legal, acesso controlado, retenção coerente, resposta a solicitações e medidas de segurança. Privacidade não é apenas mascaramento: envolve todo o ciclo de coleta, uso, compartilhamento, exportação e descarte.

4.12. 12. INCIDENTES, CONTINUIDADE E RECUPERAÇÃO

O plano de resposta deve prever perda de vídeo, acesso indevido, alteração de configuração, malware, indisponibilidade do VMS, comprometimento de credenciais, falha de storage e vazamento de imagens. O procedimento define contenção, preservação de evidências, comunicação, recuperação, validação e análise de causa.

Backups de configuração e bancos precisam ser testados. A recuperação deve considerar dependências, certificados, licenças, versões, credenciais técnicas, drivers e sequência de inicialização. Um arquivo de backup que nunca foi restaurado é apenas uma expectativa.

Segurança e disponibilidade precisam ser verificadas em conjunto.

Uma configuração restritiva que impede a operação não é sustentável; uma configuração conveniente que expõe todo o sistema também não. O projeto deve equilibrar risco, desempenho, manutenção e resposta operacional.

Conhecer a solução de Monitoramento Patrimonial

5. CHECKLIST DE HARDENING E ACEITE

O aceite de cibersegurança deve produzir evidências, não apenas declarações. A matriz abaixo resume verificações mínimas que devem ser adaptadas ao risco e às tecnologias utilizadas.

DomínioVerificaçãoEvidênciaInventárioTodos os ativos, versões, endereços e responsáveis estão registradosCadastro e diagrama atualizadoRedeZonas, ACLs e portas correspondem aos fluxos aprovadosMatriz de comunicação e testeIdentidadesContas padrão removidas, perfis mínimos e MFA aplicado quando cabívelRelatório de usuários e permissõesCâmerasHTTPS, tempo, logs, serviços e protocolos configurados pela baselineChecklist por dispositivo ou política de gestãoVMSServidores, serviços, banco e clientes seguem linha de baseRelatório de hardening e versõesCriptografiaCertificados válidos e fluxos sensíveis protegidosInventário de certificados e testesAcesso remotoNão existe exposição direta; sessões são autenticadas e registradasConfiguração da solução e logsLogsEventos relevantes possuem data, fonte, usuário e retençãoConsultas e exportação de registrosAtualizaçõesFirmware e software possuem situação de suporte e plano de correçãoMatriz de vulnerabilidades e mudançasBackupConfigurações e dados críticos podem ser restauradosRelatório de teste de recuperaçãoEvidênciasExportação preserva origem, tempo, integridade e reproduçãoArquivo de teste e cadeia de custódiaFornecedoresAcessos, suporte, vulnerabilidades e encerramento estão contratualmente definidosCláusulas, procedimentos e responsáveis

6. PLANO DE IMPLEMENTAÇÃO POR MATURIDADE

NívelPrioridadesResultadoFundaçãoInventário, troca de credenciais, atualização crítica, segmentação inicial, bloqueio de exposição direta e backupRedução dos riscos mais imediatos e visibilidade do parqueControladoPerfis individuais, baseline de hardening, ACLs, certificados, logs centrais, processo de mudanças e acesso remoto governadoArquitetura repetível e auditávelGerenciadoMonitoramento contínuo, gestão de vulnerabilidades, testes de recuperação, métricas, fornecedores e resposta a incidentesRisco acompanhado durante o ciclo de vidaResilienteDefesa em profundidade, automação de conformidade, simulações, análise de dependências e melhoria contínuaCapacidade de resistir, detectar, responder e recuperar

A sequência deve ser orientada pelo risco. Corrigir exposição pública, credenciais conhecidas, firmware vulnerável e ausência de backup costuma ser mais urgente do que implantar controles avançados em componentes de baixa criticidade.

7. MODELO DE AMEAÇAS APLICADO AO CFTV

Um programa de cibersegurança começa pela compreensão de como o sistema pode ser comprometido e quais consequências precisam ser evitadas. No CFTV, o adversário não precisa necessariamente interromper toda a plataforma. Alterar o campo de visão de uma câmera, reduzir a qualidade de gravação, modificar o relógio, excluir um intervalo, obter uma credencial de manutenção ou criar uma rota não autorizada para o storage já pode comprometer a finalidade do sistema.

O modelo de ameaças deve considerar agentes externos, usuários internos, prestadores de serviço, dispositivos comprometidos, falhas de configuração e eventos acidentais. A mesma vulnerabilidade pode produzir impactos diferentes conforme a aplicação. A indisponibilidade de uma câmera administrativa pode ser tolerável por algumas horas; a perda silenciosa de uma câmera que confirma uma manobra em uma instalação crítica pode exigir resposta imediata.

Cenário de ameaçaAtivo ou função afetadaImpacto principalControles de engenhariaEvidência de controleUso de credencial padrão ou reutilizadaCâmera, VMS, storage ou estaçãoAcesso não autorizado e perda de rastreabilidadeContas individuais, segredo único, MFA quando disponível e gestão centralizadaRelatório de contas, política aplicada e teste de autenticaçãoExploração de serviço desnecessárioDispositivo de bordaExecução remota, reconhecimento ou movimentação lateralBaseline de serviços, firewall local, segmentação e atualizaçãoInventário de portas e varredura

validadaSubstituição ou manipulação do fluxoTransmissão de vídeo e metadadosApresentação de imagem falsa ou perda de confiança na evidênciaCriptografia, autenticação de dispositivo, assinatura e monitoramento da interconexãoTeste de certificado, verificação de assinatura e evento de falhaAlteração do relógioCâmeras, VMS e registrosImpossibilidade de correlacionar eventosNTP ou NTS controlado, restrição de alteração e monitoramento de desvioRelatório de sincronismo e trilha de mudançasComprometimento de estação de operaçãoCredenciais, imagens e VMSExfiltração, alteração e propagação de malwareEstação dedicada, endurecimento, EDR compatível, menor privilégio e bloqueio de mídia removívelBaseline da estação e registros de proteçãoRansomware em servidores ou storageGravação, banco de dados e configuraçãoIndisponibilidade e perda de históricoSegmentação, backup isolado, privilégios mínimos, monitoramento e restauração testadaRelatório de restauração e teste de continuidadeAcesso remoto indevidoAdministração e suporteAlterações não rastreadas e persistência externaGateway controlado, MFA, autorização por sessão, prazo e registroLogs de sessão, aprovação e revogaçãoExportação não autorizadaImagens e metadadosVazamento de dados e quebra da cadeia de custódiaPerfis restritos, formato protegido, registro e destino controladoAuditoria de exportação e termo de custódiaFim de suporte do componenteCâmera, sistema operacional, driver ou VMSVulnerabilidades sem correção e incompatibilidadeGestão de ciclo de vida, matriz de suporte e plano de substituiçãoInventário de versões e roadmap de atualizaçãoFalha silenciosa da gravaçãoRecording server ou storageAusência de evidência apesar da aparente disponibilidadeMonitoramento de funções essenciais, testes de reprodução e capacidadeTeste amostral, alarme de falha e indicador de saúde

7.1. FRONTEIRAS DE CONFIANÇA

Cada mudança de contexto deve ser tratada como uma fronteira de confiança. A comunicação entre uma câmera e o recording server, entre o VMS e o storage, entre uma estação de operação e o servidor, entre uma API e um sistema externo ou entre um técnico remoto e a rede interna exige identidade, autorização, proteção do canal e registro.

Integração não significa confiança irrestrita. A ABNT NBR IEC 62676-1-1 trata sistemas externos como usuários do VSS, sujeitos a direitos de acesso especificados. Isso deve ser traduzido em contas técnicas dedicadas, permissões limitadas, interfaces documentadas, certificados e monitoração dos fluxos.

8. ARQUITETURA DE REFERÊNCIA SEGMENTADA

A segmentação de segurança agrupa ativos com função, criticidade e requisitos semelhantes. O método do NIST CSWP 28 pode ser adaptado ao CFTV em seis movimentos: inventariar ativos, avaliar risco, criar zonas, atribuir criticidade, mapear comunicações, definir controles e consolidar o diagrama lógico.

A quantidade de zonas deve equilibrar redução de risco e capacidade operacional. Uma rede excessivamente simples facilita movimentação lateral; uma arquitetura fragmentada sem documentação pode impedir manutenção e gerar liberações emergenciais. O desenho deve ser suficientemente granular para limitar o impacto de uma falha, mas administrável pela organização.

Zona de segurançaAtivos típicosCriticidadePrincípio de acessoBorda de vídeoCâmeras, encoders, intercoms e dispositivos analíticosVariável conforme a função da cenaComunicação somente com gestão, gravação, tempo, logs e serviços autorizadosGerenciamento e gravaçãoManagement server, recording servers, event server e bancoAltaAcesso restrito a serviços e clientes explicitamente definidosArmazenamentoStorage local, SAN, NAS, arquivo e backupAltaSem acesso direto de operadores ou câmeras quando não necessárioOperaçãoSmart clients, videowall e estações de monitoramentoMédia a altaSomente funções de operação e investigação aprovadasAdministraçãoEstações técnicas, gestão de dispositivos e ferramentas de configuraçãoMuito altaAcesso privilegiado individual, controlado e auditadoIntegraçõesControle de acesso, intrusão, analíticos, PSIM, SIEM e APIsConforme o sistema integradoContas técnicas e fluxos mínimos por interfaceAcesso remoto e DMZVPN, bastion, mobile server e gateway de suporteMuito altaAutenticação forte, autorização por sessão e ausência de rota direta às câmerasMonitoramento e registrosSyslog, SNMPv3, SIEM, monitoramento de disponibilidade e NTPAltaRecebe telemetria; administração separada do ambiente monitoradoBackup e recuperaçãoRepositório de configuração, banco e cópias protegidasMuito altaAcesso limitado, imutabilidade ou isolamento compatível com o risco

8.1. MATRIZ DE FLUXOS AUTORIZADOS

O diagrama lógico precisa ser acompanhado por uma matriz de comunicação. A matriz registra origem, destino, serviço, protocolo, porta, direção, finalidade, proprietário e condição de segurança. O princípio recomendado é negar tráfego entre zonas por padrão e liberar apenas fluxos necessários à função.

OrigemDestinoFinalidadeProteção esperadaObservaçãoCâmeraRecording serverVídeo, áudio, eventos e configuração operacionalHTTPS e fluxo protegido quando suportadoCâmera não precisa alcançar clientes de operaçãoCâmeraServiço de tempoSincronizaçãoNTP controlado ou NTS quando disponívelBloquear servidores de tempo arbitráriosCâmeraSyslog ou monitoramentoAuditoria e saúdeCanal protegido e destino restritoEvitar dependência exclusiva de log localEstação de operaçãoVMSVisualização, busca e tratamento de alarmesTLS, identidade individual e perfilSem acesso administrativo à câmeraEstação administrativaVMS e dispositivosConfiguração e manutençãoMFA, bastion e janela autorizada quando aplicávelSeparar da estação cotidiana do operadorVMSStorageGravação, leitura e arquivoAutenticação forte, protocolo atual e ACLNão expor compartilhamento a usuários comunsSistema externoAPI ou Event ServerIntegração de eventos e comandosTLS, conta técnica e escopo mínimoNão conceder privilégios administrativos globaisGateway remotoAdministraçãoSuporte e diagnósticoVPN, MFA, aprovação, tempo limitado e loggingProibir port forwarding diretoVMS e dispositivosSIEM ou monitoramentoLogs, falhas e anomaliasEnvio autenticado e retenção centralDefinir alertas e responsáveis

8.2. SEPARAÇÃO FÍSICA, LÓGICA E FUNCIONAL

VLANs isolam domínios de broadcast, mas não constituem sozinhas uma arquitetura de segurança. É necessário aplicar roteamento controlado, ACLs ou firewall, autenticação de dispositivos, monitoração e revisão periódica. Em sistemas de maior criticidade, recording servers podem possuir interfaces separadas para a rede de câmeras e para a rede de servidores e clientes, reduzindo a comunicação direta entre borda e usuários.

Serviços expostos externamente, como acesso móvel ou web, devem ser posicionados em uma zona intermediária, com controles em ambos os lados. A DMZ não deve se tornar uma ponte ampla para a rede de gravação. Cada conexão iniciada para o interior precisa ter finalidade, destino e porta conhecidos.

9. BASELINE DE HARDENING DOS DISPOSITIVOS DE BORDA

A baseline é o conjunto documentado de configurações mínimas aprovadas para determinada família de dispositivos. Ela reduz variação, facilita auditoria e permite identificar desvios. O guia de hardening do AXIS OS organiza controles em proteção padrão, endurecimento básico e endurecimento estendido, abordagem que pode ser adaptada a outras plataformas conforme suas capacidades.

9.1. IDENTIDADE E CONTAS

Cada dispositivo deve possuir credencial administrativa controlada e conta dedicada para o VMS, com privilégio suficiente apenas para as funções necessárias. A conta administrativa não deve ser utilizada continuamente para transmissão de vídeo. Acesso anônimo, visualização sem autenticação e contas genéricas compartilhadas enfraquecem a rastreabilidade.

Onde houver integração com um serviço de identidade, podem ser utilizados OAuth 2.0 ou mecanismos equivalentes, desde que a dependência e o comportamento durante indisponibilidade sejam compreendidos. A autenticação central não elimina a necessidade de contas de emergência protegidas e procedimentos de recuperação.

9.2. SERVIÇOS, PROTOCOLOS E DESCOBERTA

UPnP, Bonjour, WS-Discovery, ZeroConf, SSH, FTP, Telnet, áudio, Bluetooth, Wi-Fi, slots de armazenamento e aplicações embarcadas devem ser avaliados conforme o uso real. Serviços de descoberta podem facilitar a implantação, mas não precisam permanecer anunciando o dispositivo após o comissionamento. Interfaces físicas ou lógicas sem função devem ser desabilitadas quando a plataforma permitir.

Desabilitar serviços exige análise de dependências. LLDP ou CDP, por exemplo, podem participar da negociação e da visibilidade de energia PoE. O objetivo não é remover funções indiscriminadamente, mas justificar cada serviço ativo e documentar seu proprietário.

9.3. COMUNICAÇÃO PROTEGIDA

O acesso administrativo deve utilizar HTTPS, preferencialmente com certificado emitido por uma autoridade confiável. Quando suportado pelo VMS e pelos dispositivos, SRTP ou RTSPS protege o fluxo de mídia. IEEE 802.1X com EAP-TLS autentica o equipamento na porta de rede, e MACsec pode adicionar confidencialidade e integridade ao enlace Ethernet em cenários compatíveis.

HTTP simples e autenticação básica sem canal protegido devem ser evitados. A política criptográfica precisa considerar versões TLS, conjuntos de cifras, cadeia de confiança, compatibilidade dos clientes e capacidade de renovação dos certificados.

9.4. TEMPO, REGISTROS E MONITORAMENTO

Data e hora afetam logs, certificados, pesquisa, correlação e validade da evidência. A baseline deve definir servidores NTP ou NTS, fuso, UTC, frequência de sincronização e limite aceitável de desvio. Alterações manuais precisam ser restritas e registradas.

Logs de auditoria e acesso devem ser enviados a um servidor remoto quando a criticidade justificar. O monitoramento pode combinar syslog, SNMPv3, alertas do VMS e telemetria de rede. Reinicializações, alteração de configuração, falha de armazenamento, perda de vídeo, autenticações e bloqueios por força bruta são eventos relevantes.

9.5. INTEGRIDADE DO DISPOSITIVO E DO SOFTWARE

Recursos como sistema operacional assinado, secure boot, armazenamento seguro de chaves, identidade de dispositivo, filesystem criptografado e SBOM elevam a confiança na plataforma. Eles não substituem atualização e segmentação, mas dificultam instalação de software alterado, extração de segredos e falsificação de identidade.

Aplicações embarcadas devem possuir origem, assinatura, versão, finalidade e responsável. Componentes de terceiros ampliam a cadeia de fornecimento e precisam ser incluídos na gestão de vulnerabilidades e no inventário.

9.6. ARMAZENAMENTO DE BORDA E DESCARTE SEGURO

Cartões SD e compartilhamentos de rede podem armazenar imagens, credenciais e configurações. Quando utilizados, devem receber criptografia e política de acesso compatíveis com o risco. Na retirada do dispositivo, o reset de fábrica precisa ser concluído, e as mídias removíveis devem ser apagadas ou destruídas por método definido. O descarte não termina ao remover o equipamento da rede.

10. BASELINE DO VMS, SERVIDORES, CLIENTES E STORAGE

10.1. SERVIDORES DEDICADOS E FUNÇÕES SEPARADAS

Servidores de gerenciamento, gravação, eventos, logs, acesso móvel e banco de dados possuem superfícies e requisitos distintos. Em sistemas relevantes, devem operar em servidores físicos ou virtuais dedicados, sem softwares estranhos à função. A separação reduz conflito de recursos, dependências e impacto de uma vulnerabilidade.

Contas de serviço devem ser próprias, possuir privilégio mínimo e não permitir login interativo quando desnecessário. Administração do VMS, do sistema operacional, do

banco e do storage pode ser distribuída entre funções diferentes, reduzindo concentração de poder e fortalecendo a separação de deveres.

10.2. SISTEMA OPERACIONAL E COMPONENTES DE PLATAFORMA

A baseline de servidor inclui patches, firewall local, proteção antimalware compatível, serviços mínimos, política de execução, restrição de mídia removível, auditoria, backup e acesso administrativo por estação confiável. Componentes IIS, banco de dados e APIs também precisam de configuração própria, incluindo remoção de páginas e cabeçalhos desnecessários e desativação de métodos não utilizados.

Conexões ao banco devem utilizar autenticação integrada e validação de certificados quando suportadas. Aceitar qualquer certificado elimina a garantia de identidade do servidor, mesmo quando o tráfego está criptografado.

10.3. PERFIS DE CLIENTES E ESTAÇÕES DE OPERAÇÃO

Estações de operação devem executar somente funções necessárias. Perfis podem limitar reprodução, exportação, snapshots, áudio, PTZ, levantamento de máscaras e acesso a câmeras ou períodos específicos. A estação administrativa deve ser separada da estação cotidiana sempre que a criticidade justificar.

Salvar senhas, navegar livremente, instalar aplicações ou conectar mídias removíveis transforma a estação em um ponto de exfiltração e entrada de malware. Equipamentos móveis e clientes web devem ser gerenciados, atualizados e utilizados somente em redes e dispositivos confiáveis.

10.4. PROTEÇÃO DO STORAGE E DAS GRAVAÇÕES

O storage deve preservar capacidade, desempenho, integridade e disponibilidade. Criptografia das gravações, assinatura digital, controle de acesso, monitoramento de espaço, redundância e proteção contra exclusão precisam ser definidos em conjunto. RAID reduz impacto da falha de disco, mas não substitui backup nem protege contra ransomware ou exclusão autorizada indevidamente.

Compartilhamentos NAS devem utilizar versões atuais do protocolo, autenticação adequada, ACL restrita e rede dedicada ou controlada. O recording server deve acessar somente os caminhos necessários, e operadores não devem montar diretamente os volumes de gravação.

11. PKI E CICLO DE VIDA DOS CERTIFICADOS

Certificados digitais não são um ajuste pontual. Eles formam uma infraestrutura operacional que depende de autoridade certificadora, nomes corretos, confiança distribuída, proteção das chaves privadas, renovação e revogação. Um certificado expirado pode interromper a comunicação entre clientes, management server, recording servers, mobile server e dispositivos.

Objeto protegidoUso do certificadoProprietário operacionalControle de ciclo de vidaCâmera ou encoderHTTPS, 802.1X, identidade do dispositivo e APIsEquipe de dispositivos ou segurança eletrônicaEmissão, inventário, renovação e revogaçãoManagement serverAutenticação e criptografia com servidores e clientesAdministração do VMSNome DNS, confiança da CA, chave privada e prazoRecording serverFluxos para clientes, serviços e failoverAdministração do VMSDistribuição da cadeia e permissão da conta de serviçoMobile ou web serverAcesso de clientes remotosTI e administração do VMSCertificado público ou corporativo, renovação e teste externoBanco de dadosValidação do servidor e proteção da conexãoAdministrador de bancoCertificado verificável e remoção de confiança indiscriminadaSyslog, SIEM e serviços de tempoProteção da telemetria e autenticaçãoEquipe de segurança e redesConfiança mútua e monitoramento de expiração

A documentação deve registrar número de série, emissor, sujeito, nomes alternativos, finalidade, algoritmo, localização da chave, data de expiração, responsável e procedimento de renovação. Alertas de expiração precisam ocorrer com antecedência suficiente para teste e implantação sem interrupção.

12. GESTÃO DE ATIVOS, VULNERABILIDADES E ATUALIZAÇÕES

Não é possível proteger um componente cuja existência, versão ou situação de suporte não é conhecida. O inventário técnico deve relacionar hardware, software, firmware, drivers, plugins, licenças, certificados, aplicações embarcadas, data de instalação, garantia, suporte e criticidade.

Campo do inventárioFinalidadeFabricante, modelo e número de sérieIdentificação, garantia e rastreabilidadeEndereço, hostname, MAC, VLAN e localizaçãoCorrelação física e lógicaFirmware, sistema operacional, driver e aplicaçãoAnálise de vulnerabilidades e compatibilidadeFunção e criticidadePriorização de controles e correçõesEstado de suporte e fim de vidaPlanejamento de substituiçãoContas, certificados e integraçõesGestão de identidade e dependênciasBaseline e último desvio avaliadoControle de configuraçãoResponsável técnico e proprietário de negócioTomada

de decisão e aceitação de risco

12.1. FLUXO DE TRATAMENTO DE VULNERABILIDADES

O processo começa pela recepção de avisos dos fabricantes, CVEs, resultados de varredura e achados de auditoria. Cada item deve ser comparado com o inventário para confirmar aplicabilidade. A prioridade não depende apenas da pontuação publicada: exposição, presença de exploração conhecida, função do ativo, controles compensatórios e impacto da indisponibilidade também influenciam a decisão.

Antes da atualização, devem ser avaliadas compatibilidade entre câmera, driver, VMS, analítico e integração; necessidade de backup; janela operacional; risco de retorno; e testes posteriores. O registro deve mostrar versão anterior, versão nova, motivo, responsável, resultado e eventual plano de rollback.

12.2. VARREDURA SEM COMPROMETER A OPERAÇÃO

Scanners de vulnerabilidade podem produzir falsos positivos ou afetar dispositivos embarcados. O escopo, intensidade e janela precisam ser planejados. Resultados devem ser validados com guias do fabricante e, quando necessário, suporte técnico. Em ambientes críticos, descoberta passiva e análise de configuração podem anteceder testes ativos.

13. SEGURANÇA NA RELAÇÃO COM FABRICANTES, INTEGRADORES E SERVIÇOS

A cadeia de fornecimento participa do ciclo de vida do CFTV desde a especificação até o descarte. Fabricante, distribuidor, integrador, provedor de nuvem e empresa de manutenção podem possuir acesso a software, firmware, chaves, contas, configurações e imagens. A governança deve refletir essa dependência.

Requisito contratualQuestão a ser respondidaEvidência esperadaDesenvolvimento seguroExiste processo para prevenir, testar e corrigir vulnerabilidades?Política, certificação, práticas ou relatório do fabricanteSBOM e componentesÉ possível conhecer bibliotecas e dependências relevantes?SBOM por versão ou declaração equivalenteAvisos de segurançaComo o cliente será informado sobre vulnerabilidades?Portal, mailing, contato e SLA de comunicaçãoCorreções e suportePor quanto tempo firmware e software receberão atualizações?Política de ciclo de vida e datas de fim de suporteAcesso remotoQuem acessa, como, por quanto tempo e com qual registro?Procedimento, MFA, logs e aprovaçãoTratamento de dadosImagens, metadados ou telemetria deixam o ambiente?Mapa de dados, finalidade, localização e retençãoIncidentesQual é o canal de

resposta e cooperação?Contatos, responsabilidades e prazosEncerramentoComo acessos, segredos, licenças e dados serão revogados?Checklist de offboarding e termo de conclusão

A ABNT NBR ISO/IEC 27036 oferece uma estrutura para avaliar riscos e controles nas relações com fornecedores. No contexto de CFTV, essa estrutura deve ser combinada com os requisitos técnicos da plataforma e com a realidade de suporte em campo.

14. GRAUS DE SEGURANÇA DA ABNT NBR IEC 62676 E IMPACTO NA ARQUITETURA

A ABNT NBR IEC 62676-1-1 classifica o VSS em quatro graus de segurança conforme a combinação entre probabilidade e consequência do incidente. Essa classificação não deve ser confundida com um selo genérico de cibersegurança. Ela orienta quais funções de integridade, acesso, autenticação, monitoramento e proteção de dados precisam ser aplicadas ao sistema e registradas nos requisitos operacionais.

Um mesmo empreendimento pode possuir funções com criticidades diferentes, desde que a aplicação seja coerente e documentada. Câmeras utilizadas como apoio visual podem receber requisitos distintos daquelas que constituem medida principal de redução do risco. O grau deve ser consequência da avaliação, e não uma escolha comercial feita após a especificação.

DimensãoAplicação prática no projetoReflexo cibernéticoMonitoramento das interconexõesDetectar perda ou degradação entre componentes essenciaisSupervisão ativa, alarmes de indisponibilidade e tempo máximo de notificaçãoDetecção de violaçãoIdentificar perda de vídeo, mudança de campo de visão, obscurecimento ou substituiçãoAnalíticos de integridade, tamper físico, validação de fonte e correlação de eventosNíveis de acessoSeparar operação, administração, manutenção e configuraçãoRBAC, contas individuais, autorização adicional e menor privilégioSincronização de tempoManter coerência entre componentes e registrosNTP ou NTS controlado, UTC, monitoramento de desvio e restrição de alteraçõesAutenticação dos dadosDetectar modificação, remoção ou inserção de imagens e metadadosAssinaturas, checksums, signed video e verificação da exportaçãoProteção da confidencialidadeImpedir visualização não autorizada de dados e cópiasCriptografia, controle de exportação e proteção das chavesRegistros do sistemaPermitir reconstrução de eventos, falhas e açõesLogs protegidos, centralização, retenção e auditoriaBackup e restauraçãoRecuperar dados e configuração após falhaCópias protegidas, teste de restauração e controle de versões

15. INTEGRIDADE DA EVIDÊNCIA E CADEIA DE CUSTÓDIA

A utilidade probatória de uma gravação depende da capacidade de demonstrar origem, sequência, data, hora, integridade e forma de extração. A ABNT NBR IEC 62676 diferencia gravação original, cópia exata e exportação. A gravação original é a primeira manifestação persistente; a cópia exata preserva os dados bit a bit; e a exportação pode envolver conversão necessária para reprodução ou compartilhamento.

A exportação não deve alterar o original. Deve preservar identificação da fonte, intervalo, carimbo de tempo, ordem das imagens e metadados necessários à interpretação. Quando o formato é proprietário, o pacote precisa incluir um meio de reprodução adequado. Melhorias de brilho, contraste, nitidez ou zoom aplicadas a uma cópia de trabalho devem ser registradas e nunca substituir a gravação original.

Elemento do pacote de evidênciaFinalidadeIdentificador do caso ou incidenteRelacionar a mídia ao processo de investigaçãoOrigem e identificação das câmerasDemonstrar de onde as imagens foram obtidasPeríodo em UTC e horário localPermitir correlação com outros sistemasFormato e ferramenta de reproduçãoAssegurar acesso por terceiro autorizadoHash, assinatura ou mecanismo de autenticaçãoDetectar alteração após a extraçãoUsuário e estação que realizaram a exportaçãoPreservar responsabilidade e rastreabilidadeData, hora, finalidade e autorizaçãoDemonstrar legitimidade da açãoDestino, mídia e responsáveis pelas transferênciasRegistrar a cadeia de custódiaDescrição de conversões ou melhoriasDistinguir original, cópia exata e material de trabalhoRegistro de acesso posteriorControlar cópias, visualizações e devolução

15.1. ASSINATURA NA ORIGEM E VERIFICAÇÃO POSTERIOR

Quando a plataforma suporta vídeo assinado na origem, a câmera adiciona elementos que permitem verificar autenticidade e vincular o conteúdo ao dispositivo produtor. Esse recurso reduz a dependência de confiar apenas no storage ou no VMS, mas exige preservação da cadeia de certificados, ferramenta de validação e procedimento para interpretar o resultado.

Assinatura não impede necessariamente a cópia ou divulgação da imagem. Sua função é evidenciar origem e alteração. Confidencialidade depende de criptografia, autorização e governança do acesso.

15.2. SINCRONIZAÇÃO COMO REQUISITO FORENSE

Diferenças de poucos segundos podem alterar a interpretação quando vídeo é correlacionado com controle de acesso, intrusão, telefonia, logs de rede ou eventos operacionais. O projeto deve definir uma fonte de tempo confiável, tolerância máxima, comportamento durante perda do servidor e método de verificação. O horário sobreposto na imagem não deve ser a única referência; metadados e logs também precisam ser preservados.

16. COMISSIONAMENTO CIBERNÉTICO E ACEITE TÉCNICO

Hardening sem verificação é apenas uma intenção de configuração. O comissionamento cibernético demonstra, com evidências, que os controles definidos no projeto foram implantados e que o sistema continua cumprindo sua função operacional. Os testes precisam abranger estados normais, falhas, tentativas não autorizadas e recuperação.

FAT, SAT e testes integrados possuem finalidades diferentes. O FAT pode validar configurações, templates, versões e funções antes do campo. O SAT verifica a instalação real, a rede, os certificados, os fluxos, a alimentação e as integrações. O teste integrado confirma o comportamento entre câmera, VMS, storage, diretório, firewall, SIEM, controle de acesso e operação.

TesteProcedimento resumidoCritério de aceitaçãoEvidênciaContas padrão e anônimasTentar autenticação com credenciais de fábrica e acesso sem loginAcesso negado e tentativa registradaCaptura, log e relatórioMenor privilégioExecutar funções com perfis de operador, investigador e administradorCada perfil acessa somente funções e câmeras autorizadasMatriz de permissões e resultadosSegmentaçãoTestar comunicações permitidas e bloqueadas entre zonasSomente fluxos da matriz são aceitosRegras, testes e registros do firewallPortas e serviçosExecutar varredura controlada por tipo de ativoAusência de serviços não aprovadosRelatório validado e exceçõesCertificadosValidar cadeia, nome, expiração, revogação e comportamento com certificado inválidoConexões legítimas estabelecidas e inválidas rejeitadasInventário e capturas de testeSincronizaçãoComparar câmeras, servidores e estações com a referênciaDesvio dentro do limite definidoPlanilha de medição e logsPerda de vídeoInterromper o enlace de uma câmera controladaFalha detectada, registrada e apresentada no prazoLinha do tempo do eventoViolação da câmeraObscurecer ou reposicionar em cenário de testeEvento de tamper conforme regra aprovadaAlarmes, vídeo e registroFalha de storageSimular perda de volume ou limite de capacidadeAlarme, continuidade prevista e ausência de corrupção indevidaRelatório funcionalBackup e restauraçãoRestaurar configuração e banco em ambiente controladoSistema recuperado

com versão e parâmetros esperadosTempo, resultado e pendênciasExportação de evidênciaExportar intervalo e validar origem, tempo, assinatura e reproduçãoOriginal preservado e pacote reproduzívelPacote de teste e cadeia de custódiaAcesso remotoSolicitar sessão, autenticar, executar ação e encerrarAprovação, MFA, logging, expiração e revogação funcionaisRegistro completo da sessãoLogs centralizadosGerar login negado, alteração e reinicializaçãoEventos recebidos, correlacionados e retidosConsulta no SIEM ou syslogRecuperação de energiaInterromper e restaurar alimentação em ambiente planejadoRetorno automático sem perda indevida de configuraçãoSequência e tempos registrados

16.1. DOSSIÊ DE ACEITE

O dossiê deve consolidar requisitos, diagrama de zonas, matriz de fluxos, inventário, versões, baseline, lista de contas, certificados, regras de firewall, relatórios de varredura, testes, exceções, backups, procedimentos e responsáveis. Evidências devem ser associadas aos ativos e aos critérios, evitando pastas de capturas sem contexto.

Desvios precisam ser classificados. Uma exceção aceita deve possuir justificativa, risco residual, controle compensatório, proprietário e prazo de revisão. Pendências que comprometem autenticação, gravação, integridade, disponibilidade ou recuperação não devem ser tratadas como simples acabamento.

Cibersegurança também precisa de critérios de aceite.

O sistema somente pode ser considerado endurecido quando arquitetura, configurações, permissões, evidências, contingências e responsabilidades foram verificadas no ambiente real.

Conhecer o serviço de Parametrização e Configuração de Sistemas

17. CONTINUIDADE, BACKUP E RECUPERAÇÃO

Disponibilidade não significa apenas possuir servidores redundantes. A continuidade deve considerar captura, transmissão, gravação, pesquisa, autenticação, licenciamento, banco de dados, certificados, energia e acesso operacional. A falha de uma dependência aparentemente secundária pode impedir toda a recuperação.

17.1. RTO, RPO E DEGRADAÇÃO ACEITÁVEL

O tempo objetivo de recuperação define quanto tempo cada função pode permanecer indisponível. O ponto objetivo de recuperação define quanta configuração, evento ou gravação pode ser perdida. Esses parâmetros devem ser estabelecidos por função: transmissão ao vivo, gravação, pesquisa, administração, exportação e integrações podem possuir tolerâncias diferentes.

Também deve ser definido o modo degradado. Uma câmera pode continuar gravando em borda durante a perda do recording server; um site remoto pode operar localmente sem comunicação com a central; e uma estação reserva pode assumir funções essenciais. O modo degradado precisa ser testado, monitorado e reconciliado após a recuperação.

17.2. O QUE DEVE SER PROTEGIDO

Além das gravações, precisam ser protegidos banco de configuração, mapas, regras, perfis, usuários, certificados, chaves, licenças, plugins, drivers, documentação, scripts, parâmetros dos dispositivos e inventário. A restauração do vídeo sem a configuração necessária para localizar e interpretar as imagens pode ter utilidade limitada.

17.3. TESTE DE RESTAURAÇÃO

O teste deve verificar integridade do backup, compatibilidade da versão, dependências, sequência de recuperação, permissões, certificados e retorno das integrações. O resultado inclui tempo real, dados recuperados, perdas identificadas e ações corretivas. A periodicidade deve acompanhar criticidade e frequência de mudanças.

18. RESPOSTA A INCIDENTES DE CFTV

O plano de resposta precisa conectar equipes de segurança física, TI, redes, privacidade, jurídico, operação e fornecedores. Um incidente pode afetar simultaneamente disponibilidade do monitoramento, dados pessoais, evidências e segurança do local. A decisão de desligar, isolar ou manter um componente deve considerar o risco físico produzido pela perda da função.

CenárioContenção inicialEvidências a preservarRecuperaçãoCâmera comprometidaIsolar a porta ou zona sem ampliar a indisponibilidadeLogs, tráfego, firmware, configuração e horárioReset controlado, atualização, credenciais, certificado e validaçãoCredencial administrativa expostaRevogar conta, token e sessõesAutenticações, alterações, exportações e origensRotação, revisão de privilégios e investigação de persistênciaRansomware no VMSConter servidores e impedir propagação ao storage e

backupLogs, imagem forense, alertas e linha do tempoReconstrução limpa, restauração testada e troca de segredosExportação indevidaBloquear conta e impedir novas cópiasArquivo, destino, logs, usuário, estação e autorizaçãoAvaliação de impacto, notificações aplicáveis e correção do perfilCertificado expiradoIdentificar comunicações afetadas e evitar bypass permanenteInventário, alertas e alterações emergenciaisRenovação, distribuição, validação e revisão do monitoramentoFalha ou corrupção de storagePreservar volumes, interromper escritas destrutivas e acionar contingênciaLogs, estado dos discos, alertas e configuraçãoFailover, restauração ou reconstrução com validação da gravaçãoAcesso remoto abusivoEncerrar sessão, revogar identidade e bloquear origemGravação da sessão, comandos, arquivos e aprovaçõesRevisão do gateway, contas do fornecedor e regras de autorizaçãoManipulação de tempoRestringir alteração e preservar referências independentesLogs de NTP, eventos, relógios e gravaçõesRessincronização controlada e correção das correlações

18.1. PRESERVAÇÃO ANTES DA CORREÇÃO

Atualizar, reiniciar ou restaurar imediatamente pode destruir evidências úteis. Antes da correção, a equipe deve avaliar a necessidade de coletar logs, configuração, memória, tráfego, imagens, hashes, estado do storage e linha do tempo. A preservação deve ser proporcional ao impacto e às obrigações legais ou contratuais.

19. OPERAÇÃO SEGURA E MONITORAMENTO CONTÍNUO

O aceite estabelece uma linha de base, mas o ambiente muda continuamente. Novas câmeras são adicionadas, certificados expiram, regras são abertas, usuários trocam de função, firmware perde suporte e integrações criam novos fluxos. O monitoramento deve detectar tanto falhas de disponibilidade quanto desvios de segurança.

IndicadorObjetivoExemplo de interpretaçãoCobertura do inventárioConfirmar que ativos descobertos estão cadastradosDiferenças indicam equipamento não autorizado ou gestão incompletaAtivos sem suporteMedir exposição estruturalCrescimento exige plano de modernizaçãoVulnerabilidades fora do SLAAcompanhar risco não tratadoSeparar por criticidade e exposiçãoCertificados próximos do vencimentoEvitar indisponibilidade e bypass emergencialAlertar por janelas de 90, 60 e 30 diasContas inativas ou sem proprietárioReduzir acesso residualRevogar após validação com o responsávelTentativas de login negadasIdentificar erro, ataque ou credencial desatualizadaAnalisar volume, origem e horárioPerda de vídeo e tempo de recuperaçãoMedir disponibilidade realRepetição pode indicar rede, energia ou dispositivoFalhas de gravação e capacidadeEvitar lacunas silenciosasCorrelacionar com storage e taxa de

ingestãoSucesso de restauraçãoDemonstrar recuperabilidadeBackup sem teste não conta como controle efetivoExportações e levantamentos de máscaraMonitorar uso de dados sensíveisEventos fora do padrão exigem revisãoSessões remotas de terceirosControlar manutenção externaToda sessão deve possuir solicitação, duração e resultadoDesvios da baselineIdentificar configuração não autorizadaClassificar como mudança aprovada ou incidente

19.1. INTEGRAÇÃO COM SIEM E GESTÃO DE EVENTOS

Logs de câmeras, VMS, Windows, firewall, NAC, diretório e acesso remoto podem ser correlacionados em uma plataforma de SIEM. O valor não está apenas em centralizar dados, mas em criar casos de uso: múltiplas falhas de login, dispositivo novo na VLAN, alteração de configuração fora da janela, perda simultânea de câmeras, acesso remoto seguido de exportação ou mudança de horário.

Alertas precisam possuir prioridade, proprietário, prazo e procedimento. Um SIEM sem processo de tratamento apenas transfere o excesso de eventos para outra tela.

20. PROGRAMA DE IMPLEMENTAÇÃO EM DOZE MESES

A evolução deve combinar correções imediatas com construção de capacidade permanente. O cronograma abaixo é uma referência e precisa ser ajustado à criticidade, ao tamanho do parque e às mudanças já programadas.

HorizontePrioridadesEntregáveisPrimeiros 30 diasEliminar exposição direta, contas padrão, acessos anônimos e vulnerabilidades críticas conhecidasPlano emergencial, inventário inicial e registro de riscos imediatosAté 90 diasConsolidar inventário, versões, suporte, usuários, certificados, backups e topologiaCadastro técnico, matriz de proprietários e diagrama atualAté 180 diasImplantar zonas, matriz de fluxos, baseline de câmeras, VMS e clientes, acesso remoto governadoArquitetura aprovada, regras, templates e procedimentosAté 270 diasCentralizar logs, estruturar vulnerabilidades, fornecedores, PKI e testes de restauraçãoCasos de uso, SLAs, inventário de certificados e relatórios de recuperaçãoAté 365 diasExecutar comissionamento cibernético, simular incidentes e revisar maturidadeDossiê de aceite, exercício, indicadores e plano do ciclo seguinte

21. APÊNDICE — MATRIZ MÍNIMA DE CONTROLES

A matriz abaixo funciona como ponto de partida para projeto, auditoria ou diagnóstico. A aplicabilidade deve ser definida pelo risco, pela arquitetura e pelos recursos efetivamente suportados.

DomínioControle mínimoDocumento ou evidênciaGovernançaProprietário do sistema, da rede, dos dados e das atualizações definidosMatriz de responsabilidadesInventárioHardware, software, firmware, certificados e integrações cadastradosInventário técnicoRiscoCriticidade por função e zona documentadaMatriz de riscosArquiteturaZonas e fronteiras de confiança aprovadasDiagrama lógicoFluxosComunicações interzonas justificadas e negadas por padrãoMatriz e regras de firewallDispositivosBaseline por família e versãoTemplate e relatório de conformidadeServiçosProtocolos e interfaces não utilizados desativadosVarredura e checklistRedePortas físicas e lógicas controladas; NAC quando aplicávelConfiguração de switches e NACIdentidadesContas individuais, menor privilégio e revisão periódicaRelatório de usuários e perfisAdministraçãoEstação privilegiada ou bastion para funções críticasArquitetura e logs de acessoCriptografiaHTTPS/TLS e proteção de fluxos conforme suporteConfiguração e testePKICertificados inventariados, válidos e renováveisRegistro de certificadosTempoFonte confiável e desvio monitoradoRelatório NTP/NTSVMSServidores, serviços, clientes e banco endurecidosBaseline do VMSStorageCapacidade, redundância, criptografia e acesso controladosMemória e teste de gravaçãoLogsEventos relevantes centralizados e protegidosPolítica e consultasVulnerabilidadesAvisos, CVEs, varreduras e correções governadosRegistro de tratamentoMudançasAlterações com impacto, aprovação, teste e rollbackSolicitação de mudançaBackupConfiguração e dados críticos protegidosPolítica e inventário de cópiasRecuperaçãoRestauração testada e tempos medidosRelatório de exercícioExportaçãoPerfis, formato, integridade e custódia controladosProcedimento de evidênciaPrivacidadeFinalidade, retenção, máscaras e acesso definidosRegistro de tratamento e políticaFornecedoresSuporte, vulnerabilidades, acesso e encerramento contratadosCláusulas e procedimentoIncidentesPlaybooks, contatos e preservação estabelecidosPlano e exercíciosDescarteCredenciais, certificados e dados removidos com comprovaçãoTermo de descomissionamento

A matriz não substitui a análise técnica. Sua função é impedir que controles essenciais desapareçam entre disciplinas, fornecedores e etapas do empreendimento. Cada requisito deve possuir responsável, critério de aceite, evidência e condição de manutenção.

22. REFERÊNCIAS TÉCNICAS E DOCUMENTOS CONSULTADOS

23. CONCLUSÃO

A cibersegurança em CFTV depende de arquitetura, configuração, processos e responsabilidades. Câmeras seguras em uma rede plana continuam expostas; um VMS atualizado com contas compartilhadas continua sem rastreabilidade; gravações redundantes sem controle de acesso continuam vulneráveis a uso indevido.

O resultado esperado é um sistema no qual cada ativo é conhecido, cada comunicação possui finalidade, cada usuário possui autoridade limitada, cada mudança deixa evidência e cada falha pode ser detectada e tratada. Essa disciplina conecta segurança física, TI, privacidade e operação, preservando a utilidade do videomonitoramento ao longo de todo o ciclo de vida.

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