

GUIA DIDÁTICO

Como Estruturar um Plano de Segurança Patrimonial

Diagnóstico, gestão de riscos, controles, resposta e melhoria contínua



1 Ficha técnica

Este e-book apresenta um método prático para transformar preocupações difusas de segurança em um plano documentado, aprovado, executável e revisável. A proposta foi escrita para organizações privadas, públicas, condomínios, unidades industriais, centros logísticos, escritórios, instituições de ensino, serviços de saúde, lojas, eventos e operações com múltiplos turnos.

Como usar este material

Leia os capítulos em sequência quando estiver começando do zero. Quando já existir um plano, use os capítulos 3 a 10 para realizar um diagnóstico de lacunas e os anexos para organizar a implantação. O conteúdo deve ser adaptado ao risco, ao porte, ao local, à legislação aplicável e à capacidade real de execução da organização.

Elemento	Definição editorial
Objetivo	Oferecer um caminho de decisão, não uma lista genérica de equipamentos.
Público	Gestores, síndicos, administradores, profissionais de segurança, facilities, operações, compliance, RH, tecnologia e auditoria.
Limite	Não substitui projeto técnico, avaliação jurídica, laudo de engenharia, plano de prevenção contra incêndio ou consulta aos órgãos competentes.

Atenção

As referências legais e normativas são apresentadas para orientação educacional. A Lei nº 14.967/2024 e o Decreto nº 13.012/2026 devem ser lidos em sua redação vigente, e requisitos estaduais ou municipais podem alterar a solução adequada.

1.1 Nota de atualização

A Lei nº 14.967/2024 instituiu o Estatuto da Segurança Privada, revogou a Lei nº 7.102/1983 e passou a organizar nacionalmente os serviços de segurança privada.^[1] Em 2026, o Decreto nº 13.012 regulamentou procedimentos de autorização, controle e fiscalização e distinguiu, entre outros conceitos, plano de segurança e projeto de segurança.^[2]

2 Como ler este e-book

Segurança patrimonial não é sinônimo de vigilância armada, de câmera ou de controle de portaria. Ela é um sistema de proteção no qual pessoas, processos, tecnologia, infraestrutura e governança trabalham em conjunto para reduzir a probabilidade e o impacto de eventos indesejados.

O plano é o documento que transforma esse sistema em uma referência comum. Ele responde, com clareza, a seis perguntas: o que deve ser protegido; contra quais ameaças; em que condições; com quais responsabilidades; como a organização responderá; e como saberá se os controles estão funcionando.

Símbolo textual	Uso
Em síntese	Conclusão ou princípio que deve ser lembrado.
Atenção	Risco de interpretação equivocada, lacuna legal ou execução insegura.
Exemplo	Situação fictícia que ajuda a adaptar o método.

2.1 Resultado esperado

Ao concluir a leitura, o leitor deverá ser capaz de elaborar uma versão inicial do plano, conduzir uma reunião de validação com as áreas envolvidas, priorizar investimentos e estabelecer um ciclo de revisão. A qualidade não estará no tamanho do documento, mas na ligação entre risco, controle, responsável, evidência e prazo.

Regra de ouro

Um controle só pode ser considerado parte do plano quando existe um responsável identificado, uma forma de execução, um critério de verificação e um tratamento previsto para quando o controle falhar.



3 Sumário

1	Ficha técnica	2
1.1	Nota de atualização	2
2	Como ler este e-book	3
2.1	Resultado esperado	3
3	Sumário	4
4	Segurança patrimonial como sistema	1
4.1	Quatro confusões frequentes	1
4.2	O modelo de três perguntas	1
5	Governança, escopo e responsabilidades	2
5.1	Patrocínio e papéis	2
5.2	Escopo	2
5.3	RACI simplificado	2
6	Diagnóstico do contexto	4
6.1	Roteiro de levantamento	4
6.2	Entrevistas que geram evidência	4
6.3	Inspeção orientada por jornada	4
6.4	Produto do diagnóstico	4
7	Inventário de ativos e criticidade	6
7.1	Categorias de ativos	6
7.2	Critérios de criticidade	6
7.3	Cadastro mínimo	6
8	Ameaças, vulnerabilidades e cenários	7
8.1	Linguagem de cenário	7
8.2	Taxonomia de ameaças	7
8.3	Vulnerabilidades observáveis	7
9	Avaliação e priorização de riscos	8
9.1	Probabilidade e impacto	8
9.2	Matriz de decisão	8
9.3	Risco inerente e residual	8
10	Tratamento de riscos e defesa em camadas	9
10.1	Hierarquia de controles	9
10.2	Princípio da independência	10
11	Segurança física e desenho do ambiente	11
11.1	Perímetro e aproximação	11
11.2	Zoneamento	11
11.3	Segurança e vida	11
12	Controle de acesso e gestão de visitantes	12
12.1	Ciclo de acesso	12
12.2	Visitantes e prestadores	12
12.3	Chaves, credenciais e exceções	12

13	Sistemas eletrônicos de segurança	13
13.1	CFTV e videomonitoramento	13
13.2	Alarmes e sensores	13
13.3	Integração e cibersegurança	13
14	Pessoas, cultura e fornecedores	14
14.1	Seleção, integração e treinamento	14
14.2	Gestão de empresas contratadas	14
15	Procedimentos operacionais e registros	15
15.1	Estrutura de um procedimento	15
15.2	Rondas e inspeções	15
15.3	Gestão de mudanças	15
16	Resposta a incidentes	16
16.1	Prioridade de resposta	18
16.2	Classificação	18
16.3	Comunicação	18
17	Continuidade e recuperação	19
17.1	Análise de impacto	19
17.2	Estratégias	19
18	Proteção de dados no plano patrimonial	20
18.1	Mapa de tratamento	20
18.2	RIPD e alto risco	20
18.3	Incidentes de dados	20
19	Indicadores, auditoria e melhoria	21
19.1	Indicadores com contexto	21
19.2	Auditorias e testes	21
20	Roteiro de implementação em 90 dias	22
20.1	Correções rápidas e projetos estruturantes	22
20.2	Portfólio de ações	22
20.3	Aceitação e comunicação	22
21	Estudo de caso: Centro Logístico Aurora	23
21.1	Contexto e ativos	23
21.2	Priorização	23
21.3	Tratamento proposto	23
22	Modelo de documento do Plano de Segurança Patrimonial	24
22.1	Critérios de qualidade do documento	24
23	Checklist de diagnóstico	25
23.1	Como interpretar	25
24	Checklist de controle de acesso	26
24.1	Teste de amostragem	26
25	Matriz de riscos — modelo preenchível	27
25.1	Critérios de decisão	27
26	Plano de ação e evidências	28

26.1 Reunião de acompanhamento	28
27 Glossário essencial	29
28 Referências legais e normativas	30
29 Referências consultadas	31
30 Encerramento	32
31 Anexo A – Roteiro de entrevista com gestores	33
32 Anexo B – Roteiro de inspeção física	34
33 Anexo C – Ficha de ativo crítico	35
34 Anexo D – Registro de incidente	36
35 Anexo E – Classificação de incidentes	37
36 Anexo F – Matriz de comunicação	38
37 Anexo G – Plano de testes	39
38 Anexo H – Plano anual de treinamento	40
39 Anexo I – Programa de manutenção	41
40 Anexo J – Auditoria de fornecedores	42
41 Anexo K – Calendário de revisão	43
42 Anexo L – Autoavaliação de maturidade	44
43 Anexo M – Oficina de cenários	45
44 Anexo N – Termo de aprovação e aceite de risco	46
45 Anexo O – Guia de redação segura do plano	47

4 Segurança patrimonial como sistema

Segurança patrimonial é a capacidade organizada de proteger pessoas, instalações, informações, recursos financeiros, equipamentos, estoques, processos e reputação contra eventos que possam causar dano, interrupção, perda, exposição indevida ou responsabilidade. A definição é deliberadamente ampla: ela permite incluir tanto uma porta de acesso quanto a governança de um fornecedor de tecnologia, desde que ambos contribuam para um objetivo de proteção.

Um plano maduro não começa pela pergunta “qual equipamento comprar?”. Começa por “qual consequência a organização não pode aceitar?”. A câmera, a catraca, a ronda, o controle de chaves ou o treinamento são meios. O fim é manter a integridade das pessoas, preservar os ativos prioritários e sustentar a operação dentro de níveis aceitáveis de risco.

4.1 Quatro confusões frequentes

Confusão	Correção didática
Segurança é apenas vigilância	Vigilância pode ser uma camada, mas o plano também envolve arquitetura, processos, tecnologia, pessoas, fornecedores, continuidade e dados.
Mais tecnologia significa mais segurança	Tecnologia sem operação, manutenção, proteção lógica e resposta pode gerar falsa sensação de proteção.
Risco é o mesmo que ameaça	Ameaça é uma fonte potencial de dano; risco combina possibilidade, exposição, vulnerabilidade e consequência.

A Lei nº 14.967/2024 estabelece que a prestação de serviços de segurança privada deve observar a dignidade da pessoa humana, a proteção à vida e o interesse público.^[1] Portanto, um plano patrimonial não pode ser desenhado apenas para proteger bens materiais; ele precisa reduzir situações de exposição indevida, abuso, conflito ou resposta desproporcional.

4.2 O modelo de três perguntas

Para cada decisão, o gestor deve registrar: qual objetivo de proteção está sendo atendido; qual risco está sendo tratado; e como a organização comprovará que o controle funciona. Essa sequência evita a aquisição de soluções desconectadas e facilita a prestação de contas.

Exemplo

Uma unidade quer instalar uma câmera em uma doca. O objetivo pode ser controlar acessos fora de horário, investigar desvios e aumentar a segurança dos trabalhadores. Cada finalidade demanda enquadramento, posicionamento, retenção de imagens, responsável pelo acesso e procedimento de resposta diferentes.

5 Governança, escopo e responsabilidades

A governança do plano é o conjunto de decisões que dá legitimidade, prioridade e limites ao programa de segurança. Sem governança, o documento vira um arquivo arquivado, e cada área interpreta a proteção de forma diferente. O primeiro passo é nomear um patrocinador executivo e um responsável operacional com autoridade para coordenar as áreas.

5.1 Patrocínio e papéis

A alta administração define a tolerância ao risco, aprova recursos e resolve conflitos entre proteção, custo, experiência do cliente e continuidade da operação. O gestor de segurança traduz objetivos em controles. Operações conhece os fluxos reais. RH influencia seleção, treinamento e desligamento. Tecnologia protege a infraestrutura digital. Jurídico, privacidade e compliance orientam limites legais e contratuais.

Papel	Responsabilidade mínima no plano
Patrocinador executivo	Aprovar objetivos, prioridades, orçamento e aceitação de riscos residuais.
Gestor do plano	Manter o documento, coordenar o diagnóstico, acompanhar indicadores e propor revisões.
Responsáveis de processo	Definir controles da rotina, fornecer evidências e tratar não conformidades.

5.2 Escopo

O escopo deve especificar unidades, áreas, horários, processos, pessoas, terceiros, ativos e interfaces incluídos. É importante declarar também o que está fora do escopo e quais premissas foram adotadas. Uma instalação que compartilha portaria com outro condomínio, por exemplo, não pode ser analisada como se tivesse controle exclusivo sobre todos os acessos.

Pergunta de escopo	Registro esperado
Onde	Unidades, endereços, pavimentos, áreas externas, docas, estacionamentos e áreas críticas.
Quando	Horários de operação, turnos, períodos de menor ocupação, feriados e atividades extraordinárias.
Com quem	Empregados, visitantes, prestadores, transportadores, clientes, órgãos públicos e vizinhança relevante.

5.3 RACI simplificado

Uma matriz de responsabilidades pode usar quatro papéis: responsável por executar; aprovador; consultado; e informado. O objetivo não é burocratizar a operação, mas evitar que uma tarefa crítica dependa de uma pessoa que não foi designada.

Atividade	Executa
Aprova	Consulta
Informa	Revisar riscos
Gestor	Diretoria
Operações, RH, TI	Áreas afetadas

Testar alarme	Equipe local
Gestor	Manutenção, TI
Administração	

6 Diagnóstico do contexto

O diagnóstico descreve como a organização funciona antes de avaliar como ela deveria funcionar. A observação deve combinar documentos, entrevistas, inspeção física, registros de incidentes, dados de acesso, plantas, contratos, ordens de serviço e percepção dos usuários. Nenhuma fonte isolada é suficiente: o documento formal pode dizer que existe uma ronda, enquanto o registro de turno revela que ela não é realizada em todos os horários.

6.1 Roteiro de levantamento

Etapa	Pergunta orientadora
Preparar	Quais documentos, plantas, contratos, inventários, licenças, relatórios e registros já existem?
Observar	Como as pessoas, veículos, materiais e informações realmente circulam?
Conversar	Quais situações geram imprevisto, conflito, perda de tempo ou exposição?
Comparar	O procedimento escrito coincide com a prática e com a capacidade instalada?

6.2 Entrevistas que geram evidência

Entrevistas devem ser curtas, orientadas por fatos e realizadas com diferentes perfis. Perguntas como “o que você faria se...” revelam capacidade de resposta, enquanto “o que aconteceu na última vez...” ajuda a identificar padrões. É preferível registrar exemplos concretos a coletar opiniões genéricas sobre uma área.

Boa prática

Depois de cada entrevista, registre data, função do entrevistado, processo discutido, evidência citada, risco percebido e ação sugerida. A ata não deve expor dados pessoais desnecessários nem transformar uma percepção isolada em conclusão definitiva.

6.3 Inspeção orientada por jornada

A inspeção deve acompanhar a jornada de um usuário ou de um recurso: chegada, identificação, entrada, deslocamento, permanência, saída e registro. Em uma operação logística, a jornada do caminhão inclui agendamento, triagem, pesagem, doca, carregamento, conferência, liberação e saída. Cada transição pode criar oportunidade de erro, fraude ou acidente.

Jornada	Pontos a observar
Pessoa	Identidade, autorização, acompanhante, áreas acessíveis, necessidade de ajuda e tratamento de exceções.
Veículo	Placa, motorista, carga, lacre, documentação, rota interna, parada e devolução de recursos.
Informação	Quem visualiza, registra, copia, compartilha, armazena e elimina cada dado.

6.4 Produto do diagnóstico

O diagnóstico termina quando a organização consegue desenhar um mapa de contexto, listar ativos prioritários, apontar vulnerabilidades observadas e documentar lacunas. Ele não termina quando se visita

a instalação. A visita é apenas um dos meios para produzir uma linha de base que será atualizada no ciclo de melhoria.

7 Inventário de ativos e criticidade

Ativo é tudo aquilo que possui valor ou que sustenta um resultado desejado. Um plano patrimonial deve incluir ativos tangíveis, intangíveis e humanos. O inventário não precisa listar cada parafuso; deve registrar o nível de detalhe que permite decidir proteção, prioridade, responsável e evidência.

7.1 Categorias de ativos

Categoria	Exemplos
Físicos	Edificações, cercas, portões, máquinas, veículos, estoques, cofres, ferramentas e infraestrutura elétrica.
Humanos	Empregados, visitantes, clientes, prestadores, equipes de resposta e pessoas vulneráveis no local.
Informacionais	Imagens, registros de acesso, projetos, chaves, credenciais, dados de clientes e relatórios de incidentes.

Um ativo pode ser crítico mesmo que tenha baixo valor de reposição. A sala elétrica, o sistema de comunicação ou uma chave mestra podem não aparecer no inventário financeiro, mas sua indisponibilidade pode interromper a operação. Por isso, a criticidade deve considerar valor, substituíbilidade, tempo de recuperação, impacto legal, impacto humano e efeito sobre a continuidade.

7.2 Critérios de criticidade

Critério	Pergunta
Impacto humano	Uma falha pode expor pessoas a morte, lesão, violência ou situação de vulnerabilidade?
Impacto operacional	A indisponibilidade impede produção, atendimento, transporte, pesquisa ou serviço essencial?
Impacto reputacional	O evento pode comprometer confiança, contratos, licenças ou relacionamento com a comunidade?

7.3 Cadastro mínimo

Para cada ativo, registre identificador, localização, proprietário do processo, dependências, valor qualitativo, ameaças relevantes, controles existentes, evidência de verificação e data da última revisão. O cadastro deve ser utilizável por quem toma decisão; uma planilha com centenas de campos que ninguém atualiza é inferior a um registro menor, porém confiável.

Exemplo

Em um centro de distribuição, a doca 4 pode ser classificada como ativo de alta criticidade não pelo valor da doca, mas porque concentra fluxo de entrada, expedição, terceiros e documentação de carga. A proteção deve considerar pessoas, materiais, informação e continuidade.

8 Ameaças, vulnerabilidades e cenários

Ameaça é uma condição ou agente com potencial de causar dano. Vulnerabilidade é uma fraqueza que aumenta a possibilidade de exploração ou reduz a capacidade de resposta. Consequência é o efeito caso o evento ocorra. Cenário de risco combina esses elementos em uma narrativa verificável.

8.1 Linguagem de cenário

Um cenário bem escrito possui fonte, evento, condição, ativo afetado, consequência e controles atuais. “Roubo” é uma categoria ampla. “Durante a troca de turno, uma credencial compartilhada permite acesso não autorizado à sala de estoque de alto valor, sem registro individual e sem verificação independente” é um cenário que pode ser analisado.

Elemento	Pergunta de construção
Fonte	Quem ou o que pode provocar o evento, de forma intencional ou acidental?
Evento	O que acontece, em linguagem observável?
Condição	Em que circunstância a vulnerabilidade fica mais exposta?
Consequência	O que se perde, interrompe, danifica ou expõe?

8.2 Taxonomia de ameaças

Grupo	Exemplos de investigação
Ações intencionais	Furto, fraude, invasão, vandalismo, agressão, sabotagem, extorsão e uso indevido de credenciais.
Falhas acidentais	Erro de operação, porta destrancada, registro incompleto, colisão, perda de chave ou falha de comunicação.
Eventos naturais e técnicos	Incêndio, inundação, vendaval, queda de energia, falha de rede, calor, fumaça ou indisponibilidade de fornecedor.

A taxonomia não deve ser usada para produzir um catálogo alarmista. Ela existe para reduzir pontos cegos e orientar entrevistas. O risco de ameaça interna, por exemplo, não deve ser tratado por desconfiança generalizada, mas por segregação de funções, credenciais individuais, registros, supervisão, canais de denúncia, investigação responsável e respeito aos direitos das pessoas.

8.3 Vulnerabilidades observáveis

Procure condições como portas que não fecham, iluminação insuficiente, áreas sem visibilidade, rotinas previsíveis, chaves sem inventário, ausência de manutenção, registros que podem ser alterados, alarmes sem teste, imagens sem retenção definida, visitantes sem responsável e contratos sem exigência de evidência. O foco deve ser a condição do sistema, não a culpabilização de indivíduos.

9 Avaliação e priorização de riscos

A gestão de riscos é um processo contínuo de identificação, análise, avaliação, tratamento, monitoramento e comunicação. A ISO 31000:2018 apresenta esse ciclo como uma forma de integrar riscos à governança, estratégia, planejamento, reporte, políticas e cultura organizacional.[4] Ela também esclarece que a ISO 31000 fornece diretrizes e não é uma norma certificável.

9.1 Probabilidade e impacto

Para fins didáticos, pode-se usar escala de 1 a 5. Probabilidade deve considerar exposição, frequência, intenção, histórico, atratividade do alvo, presença de controles e facilidade de exploração. Impacto deve considerar pessoas, operação, finanças, informação, conformidade e reputação. A escala não é uma verdade matemática; é uma convenção para tornar decisões comparáveis.

Nível	Probabilidade
Impacto	1
Raro: exigiria combinação incomum de condições.	Leve: efeito localizado, reversível e sem interrupção relevante.
3	Possível: há exposição ou histórico, ainda que irregular.
Moderado: afeta processo, atendimento, custo ou confiança por período limitado.	5
Quase certo: exposição frequente ou controle muito frágil.	Grave: ameaça à vida, interrupção relevante, dano legal, financeiro ou reputacional.

9.2 Matriz de decisão

Pontuação	Tratamento sugerido
1 a 4	Aceitar ou monitorar, desde que o responsável reconheça a exposição e exista revisão programada.
5 a 9	Reduzir com medidas proporcionais e prazo definido; registrar o risco residual.
10 a 16	Priorizar plano de ação, patrocínio e acompanhamento frequente.
17 a 25	Tratar imediatamente, interromper a atividade quando necessário e escalar para decisão executiva.

A pontuação não deve substituir julgamento profissional. Dois riscos com a mesma nota podem exigir tratamentos diferentes se um envolver vida humana e outro envolver apenas atraso operacional. A organização deve declarar critérios de desempate, limites de aceitação e situações que exigem escalonamento independentemente da pontuação.

9.3 Risco inerente e residual

Risco inerente é a exposição antes dos controles considerados. Risco residual é o que permanece depois que os controles foram implantados e verificados. O plano deve registrar ambos, pois uma pontuação baixa pode ser resultado de um controle robusto ou de uma avaliação subestimada.

10 Tratamento de riscos e defesa em camadas

Tratar risco significa escolher uma combinação de decisões: evitar a atividade, reduzir probabilidade, reduzir impacto, compartilhar responsabilidades por contrato ou seguro, aceitar o risco dentro de limites ou transferir a decisão para quem possui autoridade. O plano deve registrar a escolha e a justificativa.

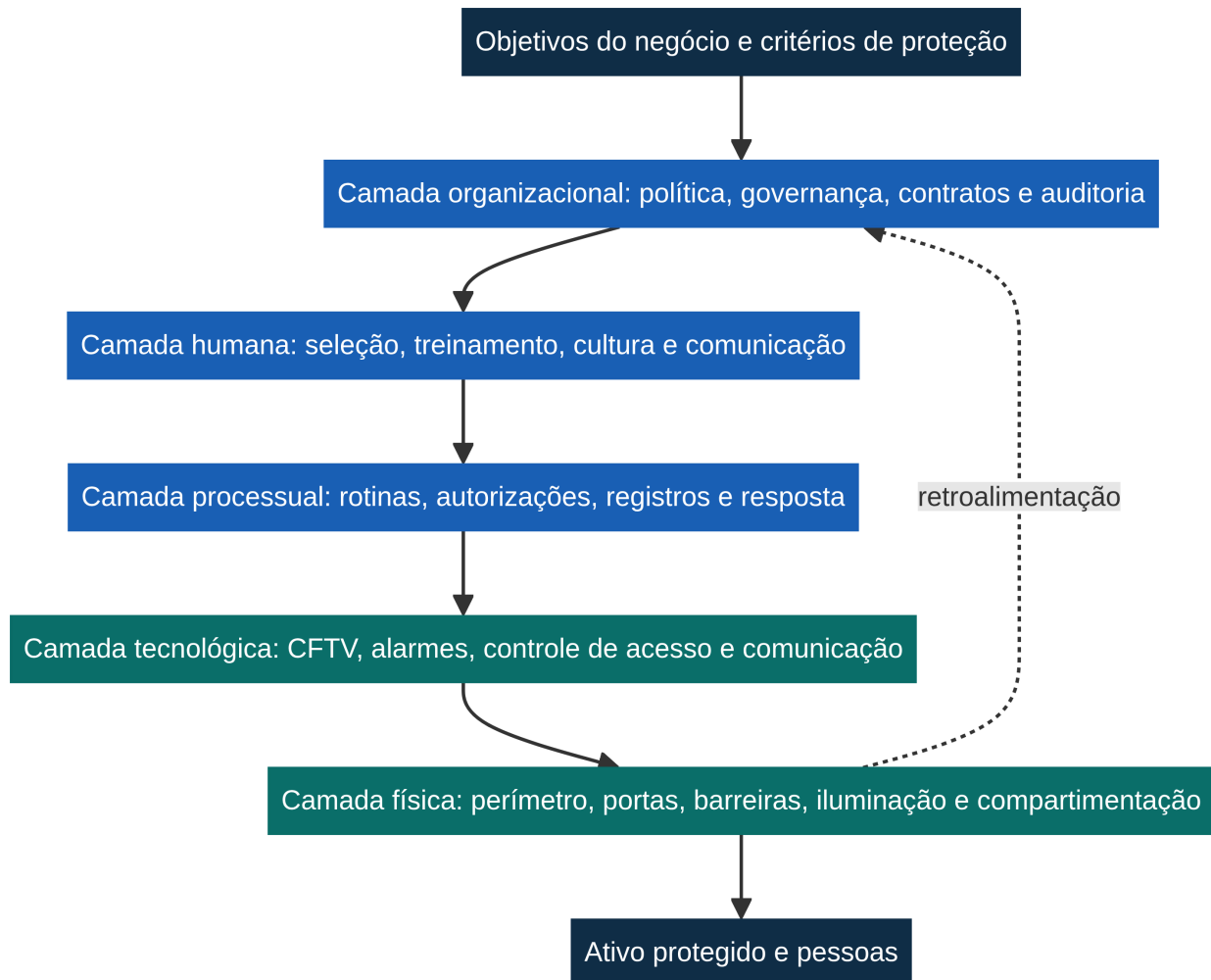


Figura 1: Defesa em camadas: objetivos, governança, pessoas, processos, tecnologia e barreiras físicas devem funcionar como um sistema.

10.1 Hierarquia de controles

Uma solução equilibrada combina controles preventivos, detectivos, reativos e de recuperação. O controle preventivo dificulta o evento; o detectivo identifica a ocorrência; o reativo orienta a resposta; o de recuperação reduz o tempo e o impacto da retomada. Quanto mais crítico o risco, mais importante é evitar depender de uma única camada.

Tipo	Pergunta
Preventivo	Como tornar o evento mais difícil ou menos atraente?
Detectivo	Como saberemos rapidamente que algo saiu do esperado?
Reativo	Quem faz o quê nos primeiros minutos e horas?
Recuperação	Como restaurar pessoas, ativos, dados e operação com segurança?

10.2 Princípio da independência

Controles independentes reduzem a chance de uma falha única derrubar toda a proteção. Um controle de acesso pode ser combinado com supervisão, registro de vídeo e revisão de exceções. Entretanto, independência não significa multiplicar barreiras indiscriminadamente. Cada camada deve ter finalidade, responsável, manutenção e critério de eficácia.

Pergunta de projeto

Se a câmera parar, qual controle ainda detectará o acesso indevido? Se a catraca liberar de forma indevida, qual processo confirmará a identidade? Se o vigilante não estiver disponível, que comunicação e procedimento assumirão a função?

11 Segurança física e desenho do ambiente

A segurança física organiza o espaço para controlar aproximação, entrada, circulação, permanência, saída e acesso a áreas críticas. O desenho deve considerar visibilidade, iluminação, barreiras, distância, tempo de resposta, rotas de fuga, acessibilidade, circulação de emergência e separação entre fluxos incompatíveis.

11.1 Perímetro e aproximação

O perímetro deve ser analisado como uma sequência de oportunidades. Uma barreira pode delimitar, retardar, direcionar e sinalizar, mas não substitui a observação e a resposta. Vegetação, entulho, equipamentos estacionados e pontos cegos podem reduzir a efetividade de cercas e câmeras.

Componente	Verificações
Perímetro	Integridade, altura, pontos de escalada, portões, iluminação, visibilidade e manutenção.
Portas	Fechamento automático, controle de chaves, resistência, sinalização, acessibilidade e saída segura.
Ambiente	Pontos cegos, áreas de espera, rotas de fuga, iluminação, ruído, identificação e circulação.

11.2 Zoneamento

Divida o local por níveis de acesso e por finalidade. Uma área pública não deve permitir passagem direta para áreas administrativas, de estoque, de tecnologia ou de operação crítica. O zoneamento facilita o controle de permissões e permite que incidentes sejam contidos antes de alcançar o ativo prioritário.

Zona	Característica
Pública	Acesso livre ou condicionado a horário, com sinalização e supervisão adequadas.
Controlada	Acesso mediante identificação, autorização e registro, com circulação limitada.
Restrita	Acesso por necessidade de saber ou fazer, com autorização específica e revisão periódica.

11.3 Segurança e vida

Barreiras, portas e procedimentos nunca podem impedir saída de emergência ou criar armadilhas. A NR-23 mantém a exigência de medidas de prevenção contra incêndio conforme a legislação estadual aplicável e obrigações relacionadas às informações aos trabalhadores e às saídas de emergência.[3]

12 Controle de acesso e gestão de visitantes

Controle de acesso é o conjunto de regras, meios e evidências que determina quem pode entrar, em quais condições, por qual rota, durante qual período e com que finalidade. A decisão deve ser baseada em autorização e necessidade, não apenas em reconhecimento visual.

12.1 Ciclo de acesso

O ciclo começa com a solicitação e termina com a revogação. Entre os extremos estão aprovação, cadastramento, emissão, entrega, uso, monitoramento, revisão, recolhimento e registro de exceções. Quando o ciclo de desligamento não é integrado ao controle de acesso, a organização mantém credenciais além do necessário.

Momento	Controle
Solicitação	Identificar pessoa, empresa, finalidade, período, áreas e responsável anfitrião.
Autorização	Confirmar necessidade, nível de acesso, prazo, condições e aprovação.
Uso	Identificar, autenticar, registrar, acompanhar exceções e responder a alertas.
Encerramento	Recolher credenciais, revogar acesso, revisar registros e comunicar pendências.

12.2 Visitantes e prestadores

O visitante deve saber onde pode estar e quem responde por sua permanência. A organização deve equilibrar acolhimento e proteção: exigências excessivas podem incentivar atalhos, enquanto ausência de controle cria exposição. Para terceiros recorrentes, é útil diferenciar acesso permanente, temporário, acompanhado e condicionado à ordem de serviço.

Procedimento mínimo

Receber a solicitação; validar identidade e finalidade; confirmar anfitrião; registrar entrada; orientar regras; emitir identificação; controlar áreas autorizadas; registrar saída; recolher identificação; tratar divergências e atrasos.

12.3 Chaves, credenciais e exceções

Chaves físicas precisam de inventário, responsável, cópia controlada, armazenamento, devolução e tratamento de perda. Credenciais digitais precisam de identidade individual, autenticação adequada, privilégio mínimo, registro, revisão e revogação. A exceção deve ser mais visível que o acesso normal: quem autorizou, por que, por quanto tempo e qual evidência será revisada.

13 Sistemas eletrônicos de segurança

Tecnologia deve ser desenhada a partir do cenário de risco. CFTV, alarmes, sensores, interfonia, controle de acesso, rastreamento e comunicação são componentes de uma arquitetura, não itens isolados. A confiabilidade depende de energia, conectividade, manutenção, configuração, proteção contra adulteração, pessoas treinadas e resposta compatível.

13.1 CFTV e videomonitoramento

O projeto deve definir finalidade, campo de visão, áreas não cobertas, qualidade, iluminação, retenção, acesso às imagens, exportação, auditoria e descarte. A câmera não deve ser posicionada apenas onde é fácil instalar; deve ser posicionada onde a evidência muda a decisão. A organização deve limitar visualização a pessoas autorizadas e documentar o tratamento de dados pessoais.

Decisão	Registro no plano
Finalidade	Prevenção, detecção, investigação, segurança de pessoas ou gestão operacional.
Cobertura	Pontos observados, limitações, áreas excluídas e justificativa.
Governança	Responsável, usuários, retenção, exportação, logs, descarte e resposta a pedidos.

13.2 Alarmes e sensores

Alarmes precisam de classificação de prioridade, confirmação, contato alternativo, teste, manutenção e protocolo de resposta. Um alerta sem capacidade de tratamento gera fadiga e perda de confiança. O plano deve diferenciar falha técnica, disparo acidental, evento confirmado, teste programado e tentativa de neutralização.

13.3 Integração e cibersegurança

Sistemas eletrônicos de controle de acesso físico combinam componentes de tecnologia da informação com portas, leitores e fechaduras. O NIST destaca que a infraestrutura de tecnologia desses sistemas também apresenta riscos cibernéticos e deve ser avaliada de forma integrada.^[12]

A ISO/IEC 27001:2022 orienta a estabelecer, implementar, manter e melhorar um sistema de gestão de segurança da informação com proteção de confidencialidade, integridade e disponibilidade.^[10] A ISO/IEC 27002:2022 oferece boas práticas de controles, incluindo acesso, criptografia, segurança de pessoas e resposta a incidentes.^[11]

14 Pessoas, cultura e fornecedores

Pessoas são parte do controle e também podem ser afetadas por ele. O plano deve proteger a equipe de segurança contra imprevisto, sobrecarga, informação insuficiente e ordens conflitantes. A cultura desejada é aquela em que relatar um desvio é mais valorizado do que escondê-lo para manter a aparência de normalidade.

14.1 Seleção, integração e treinamento

Requisitos de função, verificação permitida, integração, treinamento inicial, reciclagem e avaliação devem ser coerentes com a responsabilidade. Treinamento não é apenas palestra: deve incluir simulação, comunicação, uso de equipamentos, direitos das pessoas, preservação de evidências e limites de atuação.

Tema	Evidência esperada
Integração	Registro de orientação, conhecimento de áreas, contatos, rotas, alarmes e regras de conduta.
Competência	Treinamento, avaliação prática, validade, reciclagem e supervisão.
Cultura	Canal de relato, tratamento sem retaliação, comunicação de mudanças e reconhecimento de boas práticas.

14.2 Gestão de empresas contratadas

A Lei nº 14.967/2024 condiciona a prestação de serviços de segurança privada à autorização prévia da Polícia Federal e exige atenção à regularidade formal do prestador.[1] O Decreto nº 13.012/2026 reforça que os prestadores somente podem atuar nos serviços para os quais estejam autorizados.[2]

O contrato deve definir escopo, postos, jornada, qualificação, supervisão, substituições, equipamentos, registros, manutenção, confidencialidade, proteção de dados, incidentes, auditoria, continuidade e encerramento. Não basta contratar um preço; é necessário contratar uma capacidade verificável.

15 Procedimentos operacionais e registros

O plano descreve decisões de nível gerencial. Procedimentos transformam essas decisões em ações repetíveis. Uma boa arquitetura documental separa política, plano, procedimento, instrução de trabalho, formulário e registro. Cada nível deve ter linguagem, público, aprovação e periodicidade de revisão adequados.

15.1 Estrutura de um procedimento

Campo	Conteúdo
Objetivo	Por que a rotina existe e qual risco ela trata.
Escopo	Onde, quando e para quem se aplica.
Responsabilidades	Quem executa, supervisiona, aprova exceções e recebe comunicação.
Passos	Sequência clara, condições de parada e alternativas.

15.2 Rondas e inspeções

Uma ronda não é um passeio. Ela precisa de rota, frequência, pontos de observação, critério de desvio, comunicação, registro e escalonamento. O itinerário deve variar quando a previsibilidade criar risco, mas a variação precisa ser controlada para preservar cobertura e evidência.

Registro útil

Em vez de registrar apenas “sem alterações”, descreva a condição observada, horário, área, evidência, ação tomada e pendência. Registros repetidos e vazios não ajudam a investigar nem a melhorar.

15.3 Gestão de mudanças

Mudanças físicas, operacionais ou tecnológicas alteram o risco. A abertura de um novo turno, a chegada de um cliente, uma obra, um evento, a terceirização de uma função ou a instalação de um novo sistema devem acionar avaliação proporcional. O plano precisa ter um fluxo de mudança, ainda que simples.

16 Resposta a incidentes

Incidente é um evento que exige ação coordenada para proteger vidas, conter dano, preservar evidências, comunicar responsabilidades e restaurar a operação. A resposta precisa ser praticada antes da crise. O diagrama a seguir apresenta um fluxo geral, que deve ser adaptado ao tipo de ocorrência e às autoridades competentes.

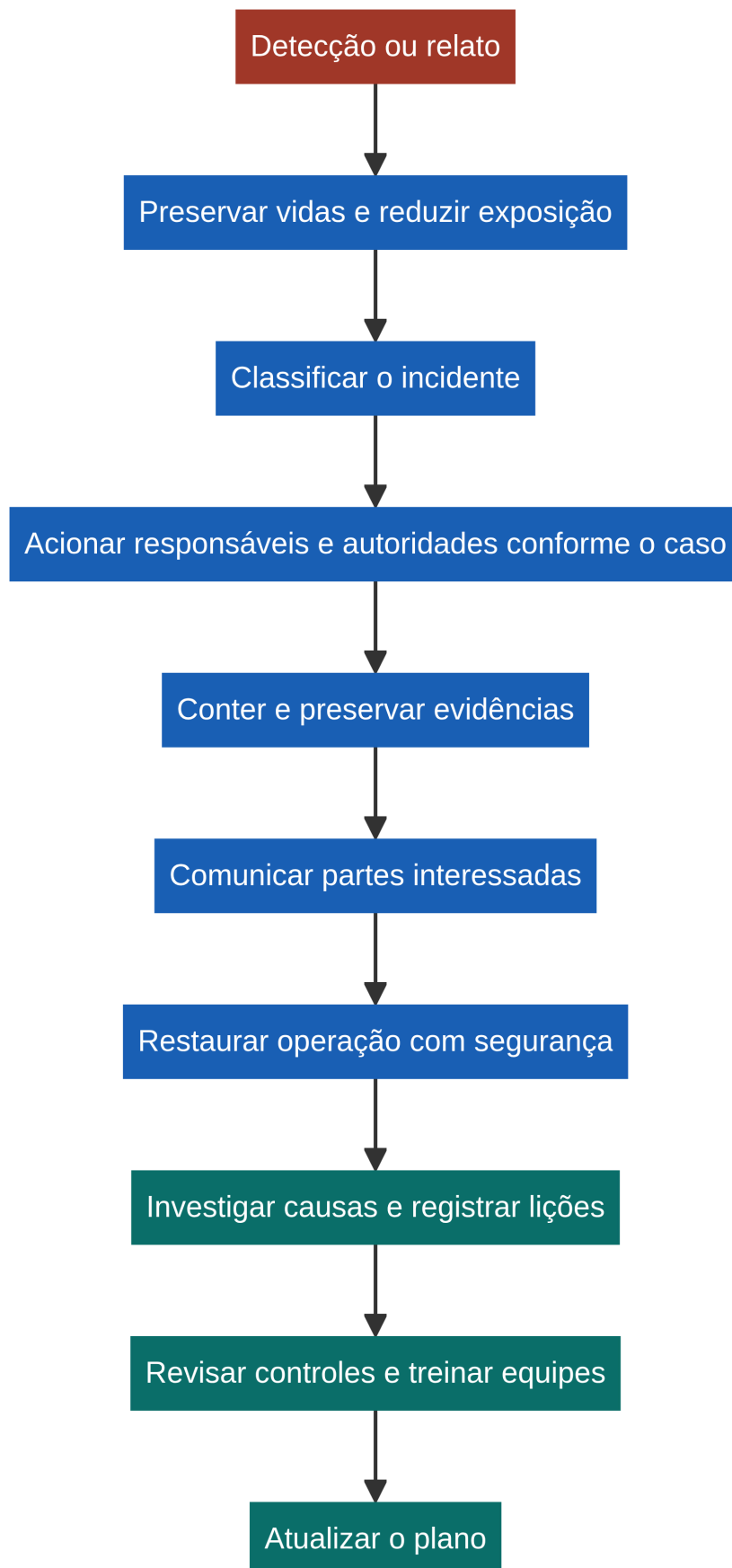


Figura 2: Fluxo geral de resposta a incidentes: preservar vidas, classificar, conter, comunicar, recuperar e aprender.

16.1 Prioridade de resposta

A primeira prioridade é proteger vidas e reduzir exposição. Depois, a equipe deve controlar o ambiente sem destruir evidências, acionar os responsáveis e as autoridades conforme o caso, comunicar com precisão e evitar especulação. A empresa não deve tentar substituir órgãos públicos ou realizar investigação para a qual não possui competência.

Momento	Perguntas
Primeiros minutos	Há risco atual para pessoas? Quem assume a coordenação? Qual área deve ser isolada? Qual comunicação é necessária?
Primeiras horas	Quais serviços precisam ser preservados? Que evidências devem ser protegidas? Quem precisa ser informado?
Após controle	O que causou o evento? Qual controle falhou? Que ação evita repetição? Quem acompanha o prazo?

16.2 Classificação

Classificação deve refletir impacto e urgência. Uma indisponibilidade de câmera pode ser baixa em um ambiente administrativo e alta em uma área de valores. A categoria do incidente determina contatos, evidências, comunicação e necessidade de acionamento do plano de continuidade.

16.3 Comunicação

Mensagens de incidente precisam ser factuais, proporcionais, autorizadas e registradas. O plano deve prever canal alternativo quando a rede estiver indisponível. Em incidentes com dados pessoais, a ANPD orienta avaliar natureza, categorias e quantidade de titulares e dados, consequências e risco, além de documentar a análise e as medidas adotadas.^[9]

17 Continuidade e recuperação

Segurança patrimonial e continuidade de negócios são disciplinas diferentes, mas dependentes. Um controle pode impedir um evento e, ainda assim, não garantir que a operação seja retomada. A ISO 22301:2019 oferece uma estrutura para planejar, implementar, operar, monitorar, revisar, manter e melhorar um sistema documentado de continuidade diante de incidentes disruptivos.[5]

17.1 Análise de impacto

A análise de impacto identifica processos prioritários, dependências, níveis aceitáveis de interrupção, recursos mínimos e consequências de atraso. O objetivo é decidir com antecedência o que deve voltar primeiro e em quais condições.

Pergunta	Aplicação
O que é essencial?	Processos, pessoas, locais, sistemas, fornecedores, equipamentos e informações sem os quais a operação não cumpre sua finalidade.
Quanto tempo é aceitável?	Tempo máximo de indisponibilidade e momento a partir do qual a consequência se torna grave.
Qual é o mínimo?	Equipe, espaço, comunicação, acesso, energia, dados e autoridade necessários para operar em contingência.

17.2 Estratégias

Estratégias podem incluir local alternativo, estoque de contingência, redundância de comunicação, procedimentos manuais, contratos de apoio, backups, equipes de sobreaviso e priorização de clientes. Cada estratégia deve ser testada; uma alternativa que existe apenas no papel não é capacidade de recuperação.

Cuidado

A continuidade não deve incentivar retorno apressado a uma área insegura. Recuperar a operação significa restabelecer atividades dentro de condições controladas, com avaliação de pessoas, ambiente, tecnologia, informação e autoridade.

18 Proteção de dados no plano patrimonial

Videomonitoramento, controle de acesso, biometria, registros de visitantes, placas, imagens, comunicações e relatórios podem envolver dados pessoais. A LGPD disciplina o tratamento de dados pessoais e protege liberdade, privacidade e livre desenvolvimento da personalidade.[6] O plano deve integrar privacidade à segurança desde o desenho, e não apenas após a instalação do sistema.

18.1 Mapa de tratamento

Para cada processo, registre quais dados são coletados, para qual finalidade, qual base legal é analisada, quem decide o tratamento, quem opera, onde os dados ficam, com quem são compartilhados, por quanto tempo e como são eliminados. A organização deve evitar coletar mais informação do que a finalidade exige.

Operação	Exemplo de decisão
Câmera	Definir finalidade, áreas, retenção, acesso às imagens, exportação e descarte.
Visitante	Registrar somente os campos necessários, informar a finalidade e limitar o acesso.
Biometria	Avaliar necessidade, proporcionalidade, alternativa, segurança reforçada e impacto sobre titulares.

18.2 RIPD e alto risco

A ANPD explica que o Relatório de Impacto à Proteção de Dados Pessoais documenta operações que podem gerar alto risco e deve conter descrição dos dados, metodologia, medidas, salvaguardas e mecanismos de mitigação.[8] Em projetos com biometria, monitoramento intenso, combinação de bases ou uso de inteligência analítica, o RIPD pode ser uma ferramenta de governança importante.

18.3 Incidentes de dados

A resposta a incidente patrimonial deve conversar com a resposta a incidente de dados. Um acesso indevido às imagens pode ser simultaneamente um evento de segurança física, um incidente de segurança da informação e uma violação de privacidade. O plano deve evitar três erros: apagar evidência, divulgar dados sem necessidade e deixar de documentar a decisão.

19 Indicadores, auditoria e melhoria

Indicador é uma medida associada a uma decisão. O plano deve preferir poucos indicadores úteis a uma coleção extensa que não produz ação. Indicadores de resultado mostram consequências; indicadores de processo mostram se os controles estão sendo executados; indicadores de capacidade mostram se a organização consegue responder.

Tipo	Exemplo
Resultado	Número e gravidade de incidentes, perdas, lesões, interrupções ou violações de acesso.
Processo	Percentual de rondas executadas, testes realizados, credenciais revisadas e treinamentos válidos.
Capacidade	Tempo de detecção, tempo de resposta, cobertura de comunicação, disponibilidade de sistemas e conclusão de planos de ação.

19.1 Indicadores com contexto

Um indicador deve possuir definição, fórmula, fonte, periodicidade, responsável, meta e ação para desvio. “Zero incidentes” pode esconder subnotificação. “Número de alarmes” pode aumentar porque a detecção melhorou. A interpretação precisa considerar exposição, mudanças operacionais, sazonalidade e qualidade do registro.

Exemplo de ficha

Indicador: percentual de credenciais revogadas até o fim do primeiro dia útil após desligamento. Fórmula: credenciais revogadas no prazo dividido por desligamentos no período. Fonte: sistema de RH e controle de acesso. Meta: 100%. Ação de desvio: análise de causa e revisão da integração entre RH, gestor e tecnologia.

19.2 Auditorias e testes

Auditoria verifica conformidade e eficácia com base em evidências. Teste verifica capacidade em uma situação controlada. Inspeção observa condição. Investigação busca causas. O plano deve distinguir os quatro usos para não tratar toda falha como problema disciplinar.

Verificação	Pergunta
Inspeção	O controle físico ou operacional está presente e em condição adequada?
Teste	O controle funciona quando acionado e a equipe sabe responder?
Auditoria	O processo é executado de forma consistente, registrada e conforme os critérios aprovados?
Revisão	O risco, o contexto ou a solução mudou a ponto de exigir atualização?

20 Roteiro de implementação em 90 dias

A implantação deve ser faseada. O objetivo dos primeiros 90 dias não é resolver todos os riscos, mas estabelecer governança, linha de base, prioridades, controles críticos e rotina de acompanhamento.

Período	Entregas
Dias 1–15	Patrocinador, escopo, equipe, mapa de ativos, documentos existentes, contatos e riscos urgentes.
Dias 16–30	Inspeções, entrevistas, cenários, matriz inicial, incidentes históricos e classificação de criticidade.
Dias 31–60	Procedimentos prioritários, correções rápidas, contratação ou adequação de controles e treinamento inicial.
Dias 61–90	Testes, indicadores, auditoria de implantação, aceite de riscos residuais e calendário de revisão.

20.1 Correções rápidas e projetos estruturantes

Correções rápidas devem ser simples, seguras, reversíveis e mensuráveis: fechar uma vulnerabilidade física evidente, corrigir uma lista de contatos, revisar uma permissão excessiva ou instituir um registro. Projetos estruturantes exigem orçamento, arquitetura, compra, obra, integração, contratação ou mudança cultural. Não se deve esconder um projeto grande dentro de uma tarefa rápida.

20.2 Portfólio de ações

Campo	Uso
Risco tratado	Vincula a ação ao cenário e evita iniciativas sem justificativa.
Responsável	Define quem conduz e quem presta contas.
Prazo e marco	Permite acompanhamento e identificação de atraso.
Evidência	Indica como a conclusão será comprovada.

20.3 Aceitação e comunicação

Ao final de cada ciclo, a direção deve saber quais riscos foram reduzidos, quais permanecem, quanto custa tratá-los e quais decisões são necessárias. Aceitar risco não significa ignorá-lo; significa reconhecer a exposição, definir responsável, prazo de revisão e condições que obrigam nova avaliação.

21 Estudo de caso: Centro Logístico Aurora

O Centro Logístico Aurora opera em dois turnos, recebe transportadores, armazena produtos de alto giro e compartilha uma rua interna com outra empresa. Possui portaria, docas, estoque, sala de tecnologia, estacionamento e área administrativa. O histórico registra divergências de carga, acesso fora de horário, falhas de rádio e períodos em que câmeras ficam indisponíveis.

21.1 Contexto e ativos

O ativo prioritário não é apenas o estoque. A operação depende do fluxo de entrada, da conferência, do sistema de gestão, das docas, das pessoas que conduzem empilhadeiras e da comunicação entre portaria e expedição. Uma falha em qualquer elo pode produzir perda, acidente ou interrupção.

Cenário	Vulnerabilidade observada
Acesso indevido à doca	Autorização por telefone sem registro e porta lateral com fechamento irregular.
Divergência de carga	Segregação insuficiente entre conferência, carregamento e liberação.
Perda de comunicação	Rádio sem teste diário e sem canal alternativo documentado.

21.2 Priorização

O cenário de acesso indevido recebeu impacto alto porque pode combinar perda material, exposição de pessoas e interrupção. O cenário de divergência recebeu prioridade alta porque a consequência financeira é recorrente e a detecção ocorre tarde. O cenário de falha de rádio recebeu prioridade média, mas foi elevado em dias de operação noturna devido à dependência de resposta rápida.

21.3 Tratamento proposto

A primeira ação foi revisar o fechamento da porta e estabelecer autorização registrada. Em paralelo, a operação separou as funções de conferência e liberação, definiu amostragem independente e implantou teste de rádio por turno. A tecnologia foi ajustada depois de validar a finalidade, a cobertura e a capacidade de resposta.

Lição do caso

O plano não começou com a compra de novas câmeras. Começou com clareza de fluxo, responsabilidade e evidência. A tecnologia entrou como camada complementar, direcionada aos cenários em que mudaria a decisão.

22 Modelo de documento do Plano de Segurança Patrimonial

O modelo a seguir pode ser copiado para um documento corporativo e adaptado. A organização deve controlar versão, aprovação, distribuição, revisão e sigilo conforme a sensibilidade do conteúdo.

Seção	Conteúdo mínimo
1. Identificação	Nome da organização, unidade, endereço, versão, proprietário, aprovadores e data.
2. Objetivos	Resultados de proteção, critérios de sucesso, princípios e limites.
3. Contexto	Escopo, operação, partes interessadas, dependências e premissas.
4. Ativos	Inventário priorizado, criticidade, responsáveis e dependências.

Seção	Conteúdo mínimo
5. Riscos	Cenários, probabilidade, impacto, controles existentes, risco residual e aceitação.
6. Controles	Camadas físicas, humanas, processuais, tecnológicas e de continuidade.
7. Procedimentos	Rotinas, rondas, acesso, chaves, alarmes, incidentes, comunicação e registros.
8. Governança	Papéis, indicadores, testes, auditorias, revisão e gestão de mudanças.

22.1 Critérios de qualidade do documento

O plano deve ser claro para quem aprova, útil para quem executa e verificável para quem audita. Deve evitar detalhes que exponham vulnerabilidades desnecessárias em cópias de circulação ampla. Informações sensíveis podem ficar em anexos controlados, mapas restritos ou procedimentos com distribuição limitada.

Atenção

Não publique mapas de pontos cegos, rotas de ronda, localização de ativos de alto valor, códigos, credenciais, contatos privados ou detalhes de contingência em uma versão aberta. O plano precisa equilibrar transparência, necessidade de saber e proteção da própria segurança.

23 Checklist de diagnóstico

Use o checklist como roteiro de conversa e inspeção. Marque “sim”, “não”, “parcial” ou “não se aplica” e registre evidência. Uma resposta “sim” sem evidência deve ser tratada como pendência de verificação.

Item	Pergunta
1	Existe patrocinador executivo e responsável pelo plano?
2	O escopo inclui unidades, horários, áreas e terceiros relevantes?
3	Existe inventário de ativos prioritários e seus responsáveis?
4	Os riscos são registrados como cenários e possuem tratamento?
5	As permissões de acesso são individuais, necessárias e revisadas?
6	Há rotina para chaves, credenciais, visitantes e prestadores?
7	CFTV, alarmes e comunicação possuem teste e manutenção?
8	Existem procedimentos para incidentes e preservação de evidências?
9	A resposta a incêndio e as saídas atendem às exigências aplicáveis?
10	Dados de acesso e imagens possuem finalidade, retenção e acesso definidos?

Item	Pergunta
11	Há treinamento inicial, reciclagem e avaliação de competência?
12	Contratos definem escopo, qualificação, registros, continuidade e auditoria?
13	Existe canal para relatar desvios e quase incidentes?
14	Indicadores possuem fórmula, fonte, responsável e ação de desvio?
15	Testes e auditorias geram planos de ação acompanhados?
16	O plano é revisado após mudança, incidente ou periodicidade definida?

23.1 Como interpretar

Se mais de um terço das respostas estiver “não” ou “parcial”, a organização deve priorizar governança, diagnóstico e controles fundamentais antes de avançar para soluções sofisticadas. O checklist não é uma certificação. Ele é um mecanismo de visibilidade para decidir onde aprofundar.

24 Checklist de controle de acesso

O controle de acesso deve ser analisado em camadas. A tabela ajuda a identificar se a organização possui apenas um dispositivo ou se possui um processo completo.

Dimensão	Pergunta de verificação
Identidade	A pessoa é identificada de modo individual e confiável para a finalidade?
Autorização	Existe aprovação, área, período, finalidade e responsável?
Autenticação	O meio de acesso é adequado, protegido e não compartilhado?
Registro	O evento é registrado com data, hora, ponto e identidade quando necessário?
Supervisão	Exceções, portas abertas, tentativas negadas e acessos fora do padrão são revisados?
Revogação	O acesso é retirado quando termina a necessidade, vínculo ou prazo?

24.1 Teste de amostragem

Escolha amostras de admissões, desligamentos, visitantes, prestadores, acessos fora de horário, tentativas negadas e chaves. Compare autorização, registro, evidência e revogação. Registre se a falha é pontual, sistêmica ou causada por ausência de integração entre áreas.

Evidência mínima

Para cada exceção, deve ser possível responder quem autorizou, por que autorizou, por quanto tempo, quais áreas foram liberadas, qual registro foi gerado e quem revisou posteriormente.

25 Matriz de riscos — modelo preenchível

A matriz deve ser preenchida com linguagem objetiva. Não use “risco de tudo”; escreva eventos observáveis e vincule cada um a um ativo e a uma consequência.

Campo	Exemplo de preenchimento
ID	R-001
Ativo	Doca e documentação de expedição
Cenário	Acesso de terceiro fora do horário sem autorização registrada
Probabilidade	3 — possível
Impacto	4 — alto
Risco inerente	12 — prioridade alta
Controles	Portaria, câmera, autorização por telefone
Lacuna	Ausência de registro único e revisão de exceções
Ação	Implantar autorização registrada e revisar acessos semanais
Responsável	Operações
Prazo	30 dias
Risco residual	6 — monitorar após teste

25.1 Critérios de decisão

A organização deve registrar por que escolheu aceitar, reduzir, compartilhar ou evitar um risco. Quando houver divergência entre áreas, a decisão deve permanecer documentada, com o risco residual explicitado. A matriz é um instrumento de gestão e não um documento para encerrar discussão.

Decisão	Quando usar
Evitar	Alterar ou interromper a atividade quando o risco não é compatível com objetivos ou limites.
Reduzir	Implantar controles proporcionais e medir se a exposição caiu.
Compartilhar	Distribuir responsabilidade por contrato, seguro ou parceria, sem abandonar supervisão.
Aceitar	Reconhecer risco residual dentro de critério aprovado e com revisão programada.

26 Plano de ação e evidências

Uma ação bem escrita conecta risco, entrega, responsável, prazo e prova de conclusão. “Melhorar segurança” não é ação. “Implantar registro individual de autorização de acesso à doca, com revisão semanal pelo supervisor de operações, até 30 de setembro” é uma ação verificável.

Campo	Exemplo
Ação	Revisar o fechamento da porta lateral e instalar sensor de posição.
Risco tratado	Acesso indevido à doca durante baixa ocupação.
Responsável	Facilities, com apoio de segurança e manutenção.
Evidência	Relatório de serviço, teste documentado, fotografia controlada e registro de exceção.
Critério de aceite	Porta fecha, sinaliza abertura e o alerta é recebido no canal correto.

26.1 Reunião de acompanhamento

A reunião deve discutir atrasos, impedimentos, risco residual, decisões necessárias e evidências. Evite gastar o tempo inteiro lendo a planilha. O gestor deve levar uma visão resumida dos riscos prioritários, das ações vencidas e das decisões pendentes.

Pergunta de encerramento

Se a ação for concluída hoje, qual evidência será produzida e qual teste mostrará que o risco foi realmente reduzido?

27 Glossário essencial

Termo	Definição operacional
Ativo	Recurso, pessoa, processo, informação ou condição que possui valor ou sustenta um resultado.
Ameaça	Fonte ou condição com potencial de causar dano, perda, interrupção ou exposição.
Vulnerabilidade	Fragilidade que aumenta a probabilidade de um evento ou reduz a capacidade de resposta.
Risco	Efeito da incerteza sobre objetivos, analisado por possibilidade e consequência.

Termo	Definição operacional
Controle	Medida que previne, detecta, responde, recupera ou demonstra uma condição de proteção.
Incidente	Evento que exige resposta coordenada para conter dano, proteger pessoas, preservar evidências ou restaurar operação.
Risco residual	Exposição que permanece depois dos controles considerados.
Criticidade	Importância relativa de um ativo ou processo para pessoas, operação, conformidade e continuidade.

Termo	Definição operacional
Plano	Documento que organiza objetivos, contexto, riscos, controles, responsabilidades e revisão.
Procedimento	Instrução documentada que transforma uma decisão em rotina executável.
Evidência	Registro verificável de que uma atividade, controle ou decisão ocorreu.
Necessidade de saber	Princípio de limitar acesso à informação ao que é necessário para a função.

28 Referências legais e normativas

A lista abaixo orienta aprofundamento. O texto integral das normas técnicas deve ser obtido por canais oficiais ou licenciados. Este e-book não reproduz normas protegidas por direitos autorais.

Referência	Como usar no plano
Lei nº 14.967/2024	Estatuto da Segurança Privada e da Segurança das Instituições Financeiras; base para serviços, princípios e autorização.
Decreto nº 13.012/2026	Regulamenta autorização, controle e fiscalização e define projeto e plano de segurança em contextos específicos.
NR-23	Proteção contra incêndios, informação aos trabalhadores, saídas e articulação com legislação estadual.
LGPD – Lei nº 13.709/2018	Dados pessoais em acesso, imagens, biometria, visitantes, registros e incidentes.

Referência	Como usar no plano
ISO 31000:2018	Princípios, estrutura e processo de gestão de riscos; usar como orientação, não como certificação.
ISO 22301:2019	Continuidade de negócios, recuperação e melhoria da resiliência.
ISO/IEC 27001:2022	Sistema de gestão da segurança da informação e proteção de confidencialidade, integridade e disponibilidade.
ISO/IEC 27002:2022	Boas práticas de controles de segurança da informação, acesso e incidentes.

Atenção

A aplicação concreta depende do tipo de instalação, município, estado, atividade, contrato, população exposta, licenças e autoridade competente. Sempre verifique a versão vigente e as exigências locais antes de aprovar o plano.

29 Referências consultadas

Nº	Fonte
1	Lei nº 14.967, de 9 de setembro de 2024 — Câmara dos Deputados. https://www2.camara.leg.br/legin/fed/lei/2024/lei-14967-9-setembro-2024-796214-publicacaooriginal-172963-pl.html
2	Decreto nº 13.012, de 9 de junho de 2026 — Planalto. https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2026/decreto/d13012.htm
3	Norma Regulamentadora nº 23 — Portal Gov.br. https://www.gov.br/trabalho-e-emprego/pt-br/aceso-a-informacao/participacao-social/conselhos-e-orgaos-colegiados/comissao-tripartite-partitaria-permanente/normas-regulamentadora/normas-regulamentadoras-vigentes/norma-regulamentadora-no-23-nr-23

Nº	Fonte
4	ISO 31000:2018 — Risk management — Guidelines. https://www.iso.org/standard/65694.html
5	ISO 22301:2019 — Security and resilience — Business continuity management systems. https://www.iso.org/standard/75106.html
6	Lei nº 13.709/2018 — Lei Geral de Proteção de Dados Pessoais — Planalto. https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

Nº	Fonte
7	ANPD — Guia orientativo sobre segurança da informação para agentes de tratamento de pequeno porte. https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia-orientativo-sobre-seguranca-da-informacao-para-agentes-de-tratamento-de-pequeno-porte
8	ANPD — Relatório de Impacto à Proteção de Dados Pessoais. https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/relatorio-de-impacto-a-protecao-de-dados-pessoais-ripd
9	ANPD — Incidentes de segurança com dados pessoais. https://www.gov.br/anpd/pt-br/semana-da-protecao-de-dados-2022/incidentes-de-seguranca-com-dados-pessoais

Nº	Fonte
10	ISO/IEC 27001:2022 — Information security management systems — Requirements. https://www.iso.org/standard/27001
11	ISO/IEC 27002:2022 — Information security controls. https://www.iso.org/standard/75652.html
12	NIST — Electronic Physical Access Control Systems. https://csrc.nist.gov/projects/risk-management/sp800-53-controls/overlay-repository/government-wide-overlay-submissions/physical-access-control-systems

30 Encerramento

Estruturar um Plano de Segurança Patrimonial é organizar escolhas. A organização precisa decidir o que é essencial, quais riscos aceita, quais controles financia, como responde a falhas e como aprende com o que acontece. O documento é importante, mas a capacidade de execução é decisiva.

Um plano útil é específico sem revelar vulnerabilidades desnecessárias, técnico sem ser incompreensível, rigoroso sem ser impraticável e vivo sem perder rastreabilidade. Ele une o olhar de quem opera, de quem cuida das pessoas, de quem protege dados, de quem mantém instalações, de quem responde a incidentes e de quem toma decisões.

Mensagem final

Proteção patrimonial não é a promessa de que nada acontecerá. É a capacidade de reduzir exposição, reconhecer sinais, agir com responsabilidade, recuperar a operação e melhorar continuamente.

Fim do e-book

31 Anexo A — Roteiro de entrevista com gestores

Use este roteiro para compreender objetivos, dependências, tolerância a interrupções e decisões que não podem ficar implícitas. As respostas devem ser consolidadas por processo, não apenas por pessoa entrevistada.

Pergunta	O que observar na resposta
Qual resultado este processo precisa entregar?	Identificar o objetivo operacional e o impacto de uma falha.
Quais pessoas, sistemas, locais e fornecedores são indispensáveis?	Mapear dependências e pontos únicos de falha.
Que evento já causou perda, atraso ou conflito?	Diferenciar risco percebido, histórico e evidência disponível.
Qual decisão precisa de apoio executivo?	Identificar obstáculos de orçamento, autoridade, contrato ou prioridade.

Ao terminar, solicite ao gestor que escolha os três riscos que mais comprometem o objetivo do processo. Se a lista crescer indefinidamente, peça que os riscos sejam comparados por consequência, urgência e capacidade de tratamento. Essa conversa transforma preocupação em prioridade.

Registro recomendado

Nome do processo, gestor entrevistado, data, documentos consultados, riscos citados, evidências, dependências, decisões pendentes e data combinada para validação.

32 Anexo B — Roteiro de inspeção física

A inspeção deve ser realizada com segurança, sem testar barreiras de maneira arriscada ou interferir na operação. Quando um teste puder expor pessoas ou ativos, ele deve ser planejado e autorizado.

Área	Verificações
Perímetro	Integridade, iluminação, vegetação, pontos de escalada, portões, visibilidade e manutenção.
Portaria	Identificação, espera, barreira, comunicação, registros, acessibilidade e tratamento de exceções.
Áreas críticas	Zoneamento, portas, chaves, credenciais, supervisão, alarmes, câmeras, redundância e evidências.
Rotas de emergência	Sinalização, desobstrução, iluminação, portas, comunicação e compatibilidade com prevenção contra incêndio.

A inspeção deve registrar condição, localização, evidência, risco associado, correção imediata possível, ação estruturante e responsável. Fotografias controladas podem apoiar o relatório, mas devem ser armazenadas de modo compatível com a sensibilidade da informação e com a proteção de dados.

33 Anexo C — Ficha de ativo crítico

Campo	Preenchimento
Identificador	Código ou nome controlado do ativo.
Localização	Unidade, área, sala, pavimento ou rota.
Responsável	Gestor do processo ou proprietário da informação.
Dependências	Energia, rede, pessoas, fornecedor, documento ou outro ativo.
Criticidade	Baixa, média, alta ou crítica, com justificativa.
Ameaças	Cenários relevantes, sem detalhar vulnerabilidades em cópias abertas.
Controles	Medidas existentes, estado, evidência e periodicidade de verificação.
Revisão	Data, revisor e motivo da atualização.

O cadastro deve ser revisado quando houver mudança de local, processo, proprietário, tecnologia, contrato, ameaça ou consequência. A ficha também pode registrar o que não deve ser feito, como bloquear uma saída, desligar um equipamento crítico ou compartilhar uma chave mestra sem autorização.

34 Anexo D — Registro de incidente

Campo	Orientação
Identificação	Número, data, hora, local, pessoa que comunicou e responsável pelo registro.
Descrição factual	O que foi observado, sem especulação, julgamento ou atribuição precipitada de culpa.
Proteção imediata	Ações para preservar vidas, reduzir exposição, isolar área e acionar recursos.
Evidências	Registros, imagens, objetos, testemunhos e documentos preservados conforme orientação competente.
Comunicação	Quem foi informado, quando, por qual canal e qual decisão foi tomada.
Encerramento	Causa provável, impacto, ações corretivas, lições, responsável e prazo de revisão.

O registro deve ser preenchido o mais próximo possível do fato, com linguagem objetiva. Relatos sensíveis devem ter acesso limitado. A organização deve preservar a integridade do registro e evitar editar a narrativa original sem registrar a correção e a justificativa.

35 Anexo E — Classificação de incidentes

A classificação ajuda a mobilizar recursos sem transformar todo desvio em emergência. Os critérios devem ser aprovados pela organização e ajustados ao contexto local.

Classe	Características
Classe 1 — desvio	Não há dano relevante nem risco atual; requer registro, correção simples e análise de tendência.
Classe 2 — incidente	Há impacto limitado, necessidade de coordenação local, preservação de evidência e comunicação ao gestor.
Classe 3 — grave	Há risco elevado a pessoas, interrupção relevante, perda significativa, possível crime ou necessidade de autoridade externa.
Classe 4 — crise	Há ameaça ampla, múltiplas áreas afetadas, continuidade comprometida ou necessidade de comando executivo.

A classe pode ser elevada quando novas informações surgirem. A primeira classificação é uma decisão operacional, não um diagnóstico definitivo. O plano deve indicar contatos, autoridade para elevar classe e forma de registrar a mudança.

36 Anexo F — Matriz de comunicação

A comunicação deve ser planejada por público, finalidade, canal e autoridade. O princípio é informar o necessário, no tempo adequado e sem ampliar a exposição.

Público	Mensagem e canal
Equipe local	Instrução operacional curta, canal primário e alternativo, confirmação de recebimento.
Gestor executivo	Impacto, decisão necessária, risco residual e previsão de atualização.
Clientes ou comunidade	Mensagem factual, orientação de segurança, canal de dúvidas e porta-voz autorizado.
Autoridade pública	Informações solicitadas, preservação de evidências e cooperação conforme a competência.

Depois do incidente, registre o que foi comunicado e quais dúvidas se repetiram. Se a mesma pergunta aparecer várias vezes, o plano de comunicação precisa de uma mensagem mais clara ou de um canal melhor definido.

37 Anexo G — Plano de testes

Testar é observar capacidade em condições controladas. O teste deve ter objetivo, escopo, participantes, critérios de sucesso, riscos do próprio exercício, autorização, evidências e reunião de lições aprendidas.

Teste	Exemplo
Controle de acesso	Simular desligamento e verificar revogação no prazo, registro e tratamento da exceção.
Alarme	Realizar teste programado, confirmar recebimento, tempo de resposta, comunicação e retorno à normalidade.
Comunicação	Testar canal alternativo e confirmação de recebimento em horário de menor ocupação.
Continuidade	Executar procedimento manual por período definido e avaliar recursos mínimos.

Critério de sucesso

Um teste só termina quando o objetivo foi medido e as falhas receberam responsável e prazo. A ausência de incidente durante o exercício não prova que o controle é eficaz.

38 Anexo H — Plano anual de treinamento

O treinamento deve acompanhar risco e função. Pessoas que autorizam acessos, operam sistemas, recebem visitantes, supervisionam turnos ou respondem a incidentes precisam de conteúdos diferentes.

Público	Conteúdo essencial
Todos os trabalhadores	Política, canais de relato, regras de acesso, emergência, privacidade e conduta.
Portaria e recepção	Identificação, visitantes, prestadores, exceções, comunicação, conflitos e registros.
Supervisores	Escalonamento, indicadores, investigação inicial, preservação de evidências e gestão de mudanças.
Tecnologia e manutenção	Disponibilidade, testes, acessos administrativos, registros, fornecedores e continuidade.

Registre presença, conteúdo, instrutor, avaliação e necessidade de reciclagem. Aprendizagem deve ser reforçada após incidentes, mudanças de processo, alterações de tecnologia ou identificação de erro recorrente.

39 Anexo I — Programa de manutenção

Controles físicos e eletrônicos perdem eficácia quando a manutenção é reativa e sem evidência. O programa deve combinar inspeção visual, teste funcional, manutenção preventiva, correção, peça sobressalente, contato de fornecedor e verificação de retorno.

Ativo	Periodicidade a definir
Portas e fechaduras	Inspeção de fechamento, alinhamento, travas, sinalização e saída segura.
Câmeras	Imagem, foco, cobertura, iluminação, armazenamento, data e hora, acesso e exportação.
Alarmes	Disparo, comunicação, energia, bateria, zonas, logs, acionamento e resposta.
Rádios e comunicação	Bateria, alcance, canal, ruído, acessórios e canal alternativo.

A periodicidade deve considerar criticidade, ambiente, recomendação técnica, histórico de falhas e exposição. Um controle crítico não deve depender apenas da existência de um contrato de manutenção; a organização deve verificar a execução e o resultado.

40 Anexo J — Auditoria de fornecedores

A avaliação de fornecedores deve ser proporcional ao risco e ao acesso concedido. O objetivo é conhecer capacidade, regularidade, continuidade e tratamento de informações, sem exigir documentos irrelevantes ou impossíveis de manter atualizados.

Tema	Perguntas
Regularidade	A empresa e os profissionais possuem autorização, licenças, qualificações e registros aplicáveis?
Capacidade	Há supervisão, cobertura de faltas, treinamento, equipamento, comunicação e suporte?
Contrato	Escopo, indicadores, registros, confidencialidade, proteção de dados, auditoria e encerramento estão definidos?
Continuidade	Existe substituição, contingência, contatos alternativos e plano para indisponibilidade?

A auditoria deve produzir classificação, achados, prazo de correção e decisão sobre continuidade. Não se deve solicitar credenciais ou informações pessoais além do necessário para validar a capacidade e cumprir requisitos legais.

41 Anexo K — Calendário de revisão

O plano deve possuir gatilhos de revisão ordinários e extraordinários. A periodicidade pode ser anual, semestral ou mais frequente, conforme criticidade e mudança do contexto.

Gatilho	Ação
Mudança operacional	Reavaliar ativos, fluxos, horários, terceiros, acessos e controles antes da mudança entrar em produção.
Incidente ou quase incidente	Registrar lições, revisar cenário, verificar causa e atualizar procedimentos.
Alteração legal ou contratual	Validar requisitos, responsabilidades, registros e comunicação.
Falha repetida	Aprofundar causa, revisar indicador, testar solução e escalar decisão.

Uma reunião de revisão deve terminar com versão do documento, decisões aprovadas, riscos residuais, mudanças de responsabilidade e calendário de acompanhamento. Sem esses registros, a revisão vira conversa sem efeito operacional.

42 Anexo L — Autoavaliação de maturidade

A maturidade não é uma competição. Ela indica quão previsível, integrada e verificável é a capacidade de proteção. Uma organização pode ter maturidade alta em controle de acesso e baixa em continuidade, por exemplo.

Nível	Descrição
1 — inicial	Ações reativas, dependência de pessoas-chave, pouca documentação e evidência irregular.
2 — organizado	Há procedimentos básicos, responsáveis e controles, mas a execução é desigual.
3 — controlado	Riscos priorizados, indicadores, testes e auditorias orientam decisões.
4 — integrado	Segurança, continuidade, tecnologia, privacidade, pessoas e operação trabalham com objetivos comuns.
5 — adaptativo	A organização aprende com dados, mudanças, quase incidentes, exercícios e revisões sistemáticas.

Para cada dimensão, registre nível atual, evidência, lacuna, próxima capacidade desejada e prazo. A maturidade deve ser avaliada com humildade: declarar uma lacuna de forma precisa é mais útil do que atribuir um nível alto sem demonstração.

43 Anexo M — Oficina de cenários

Reúna representantes de segurança, operação, facilities, RH, tecnologia, privacidade e comunicação. Escolha um processo crítico e formule cenários sem buscar culpados. O objetivo é testar decisões e descobrir dependências invisíveis.

Rodada	Pergunta
1. Contexto	O que mudou no ambiente, no processo ou na exposição?
2. Evento	Qual ocorrência observável pode comprometer o objetivo?
3. Primeira resposta	O que precisa acontecer nos primeiros minutos para proteger pessoas?
4. Recuperação	Como o processo será retomado e quais condições precisam estar presentes?
5. Aprendizado	Qual controle, treinamento, contrato ou comunicação deve ser alterado?

Ao final, não transforme todos os cenários em projeto. Selecione os que possuem maior consequência, recorrência, exposição ou dependência crítica. A oficina é um mecanismo de aprendizagem e priorização.

44 Anexo N — Termo de aprovação e aceite de risco

O aceite de risco deve ser específico. A assinatura não elimina o risco nem transfere automaticamente toda a responsabilidade; ela demonstra que a autoridade competente conheceu a exposição, a justificativa, os controles existentes e o plano de revisão.

Campo	Preenchimento
Risco aceito	Identificação do cenário, ativo, consequência e pontuação.
Controles existentes	Medidas implantadas, limitações, evidências e dependências.
Justificativa	Por que o tratamento não será executado agora ou por que a exposição é tolerável.
Condições	O que fará o aceite deixar de ser válido.
Responsável	Nome, função, data de revisão e autoridade de aprovação.

Recomenda-se anexar o plano de ação para os riscos que não foram completamente reduzidos. O aceite deve ter vencimento ou gatilho de revisão; riscos aceitos indefinidamente tendem a desaparecer do campo de decisão.

45 Anexo O — Guia de redação segura do plano

O plano deve ser claro sem funcionar como manual de exploração da instalação. Use linguagem suficiente para orientar responsáveis e auditar controles, mas restrinja detalhes operacionais sensíveis por necessidade de saber.

Evite	Prefira
Lista pública de pontos cegos	Registro restrito de cobertura, limitações e controles compensatórios.
Código ou senha no plano	Referência a cofre de credenciais e procedimento controlado.
Descrição detalhada de rotina de resposta	Papéis, critérios e contatos em versão controlada.
Acusação sem evidência	Relato factual, preservação de evidências e investigação competente.

A revisão editorial deve verificar consistência de termos, versão, responsáveis, links, tabelas, sigilo, linguagem respeitosa e compatibilidade entre plano e procedimento. Um documento bem escrito reduz ambiguidade e também reduz a chance de execução improvisada.



www.mmuniztreinamentos.com.br