CÓDIGO INSTITUCIONAL • VGF-SEG-004 • VERSÃO 2.0

Política de Segurança da Informação, Cibersegurança e Cloud Computing

ISO/IEC 27001:2022 • ISO/IEC 27002:2022 • práticas de mercado

Requisitos mínimos para proteger informações, serviços jurídicos, pessoas e operações contra perda, indisponibilidade, alteração, vazamento e uso indevido.

ORGANIZAÇÃO	VOLK E GIFFONI FERREIRA SOCIEDADE DE ADVOGADOS — CNPJ 23.637.778/0001-01
ELABORAÇÃO	Time Técnico Operacional • 9 de outubro de 2025
APROVAÇÃO	Diretoria e Comitê multidisciplinar
SITUAÇÃO	Aprovado • uso institucional e comunicação ao mercado

Nota de integridade documental. Este instrumento estabelece compromissos e requisitos de governança. Alinhamento normativo não significa certificação, atestado de conformidade ou prova isolada de implementação.

1. Controle e identificação do documento

Campo	Informação
Título	Política de Segurança da Informação, Cibersegurança e Cloud Computing
Código	VGF-SEG-004
Versão vigente	2.0
Data de elaboração/revisão	9 de outubro de 2025
Elaboração	Time Técnico Operacional
Aprovação	Diretoria e Comitê multidisciplinar
Periodicidade de revisão	Anual ou antes, diante de alteração legal, normativa, operacional, tecnológica ou de risco relevante
Classificação	Público institucional, ressalvados anexos e evidências operacionais classificados
Proprietário do documento	Gestão de Tecnologia e Segurança da Informação

1.1 Histórico de versões

Versão	Data	Síntese da alteração	Aprovação
1.0	5 de maio de 2025	Emissão inicial e estruturação dos compromissos institucionais.	Diretoria
2.0	9 de outubro de 2025	Ampliação de SGSI, ativos, identidade, vulnerabilidades, logs, desenvolvimento seguro, nuvem, continuidade, incidentes e rastreabilidade técnica. Inclusão de fluxo executivo ilustrado e catálogo ampliado de requisitos, controles e evidências.	Diretoria e Comitê multidisciplinar

LEITURA CORRETA A versão 2.0 substitui versões anteriores. Cópias impressas são não controladas; a validade deve ser conferida no repositório oficial.

2. Objetivo, escopo e aplicação

Esta Política estabelece o Sistema de Gestão de Segurança da Informação (SGSI) da VGF, orientado a risco e melhoria contínua, preservando confidencialidade, integridade, disponibilidade, autenticidade, rastreabilidade, privacidade, resiliência e sigilo profissional em ambientes locais, remotos e de nuvem.

Aplica-se à Diretoria, sócios, advogados, estagiários, empregados, prestadores, correspondentes, consultores, parceiros e terceiros que atuem em nome ou no interesse da VGF, observadas a natureza do vínculo, as responsabilidades contratuais e a legislação aplicável. Também orienta a relação com clientes, titulares de dados, fornecedores, autoridades, comunidade e demais partes interessadas.

- Abrange informações de clientes, casos, partes, pessoas, finanças, estratégia, propriedade intelectual, credenciais, logs e dados públicos sob custódia.
- Abrange dispositivos, redes, aplicações, SaaS, IaaS/PaaS, APIs, correio, colaboração, backups, mídias, instalações e serviços de terceiros.
- Requisitos técnicos específicos de contratação devem ser confirmados por arquitetura, contrato e teste; esta Política não declara suporte a funcionalidade ou certificação inexistente.

HIERARQUIA Em caso de conflito, prevalecem a lei, as normas profissionais da OAB, decisões de autoridade competente e obrigações contratuais mais protetivas. Dúvidas devem ser elevadas ao proprietário do documento antes da ação.

3. Fundamentos, princípios e responsabilidades

3.1 Fundamentos e princípios

Controles são selecionados com base em risco, obrigação, criticidade, classificação e custo proporcional. Conveniência não prevalece sobre sigilo profissional e segurança mínima.

- confidencialidade, integridade, disponibilidade e resiliência;
- zero trust, menor privilégio, necessidade de conhecer e segregação;
- defesa em profundidade, configuração segura e secure by design;
- registro, monitoramento, detecção e resposta tempestiva;
- continuidade, recuperação testada e dependência gerenciada;
- responsabilidade compartilhada na nuvem e melhoria contínua.

3.2 Estrutura de responsabilidades

Papel	Responsabilidades centrais	Prestação de contas
Diretoria	Aprovar SGSI, apetite a risco, recursos e riscos residuais críticos.	Análise crítica e decisões.
Gestão de Segurança/TI	Operar controles, monitorar, responder, orientar arquitetura e manter evidências.	Indicadores, testes, incidentes e planos.
Proprietário da informação/sistema	Classificar, autorizar acessos, definir criticidade, retenção e requisitos.	Revisões de acesso, risco e continuidade.
Usuários privilegiados	Administrar de forma segregada, rastreável e limitada.	Contas nominativas, logs e revisão independente.
Fornecedores de tecnologia	Cumprir contrato, segurança, notificação, continuidade e devolução.	SLA, relatórios, atestados e testes.
Todos os usuários	Proteger credenciais, dispositivos, informação e comunicar eventos.	Treinamento, aceite e conduta.

3.3 Fluxo executivo de aplicação

O fluxo abaixo resume a sequência decisória esperada. Ele não substitui os procedimentos específicos, mas orienta o leitor sobre quando registrar, consultar, controlar, escalar e aprender.

Figura 1 — Fluxo executivo de resposta a incidentes de segurança.

4. Diretrizes institucionais

O SGSI deve manter escopo, ativos, riscos, controles, objetivos e evidências proporcionais. A declaração de aplicabilidade e o plano de tratamento orientam implementação e exceções.

4.1 Inventário e propriedade de ativos

Ativos físicos, virtuais, de nuvem, software, informação e serviços devem possuir proprietário, criticidade, localização, status e autorização.

- Atualizar inventário continuamente e revisar ao menos semestralmente.
- Detectar ativos desconhecidos e impedir conexão não autorizada.
- Registrar ciclo de vida, suporte, versão, licenciamento e descarte.

4.2 Classificação e manuseio da informação

Informações são classificadas como Pública, Interna, Confidencial ou Altamente Restrita, considerando sigilo profissional, dados pessoais, contrato e impacto.

- Rotular quando necessário e definir armazenamento, transmissão, compartilhamento, impressão e descarte.
- Restringir dados de caso e estratégia por equipe e conflito.
- Aplicar DLP ou controles equivalentes conforme risco.

4.3 Identidades, contas e autenticação

Cada usuário deve possuir identidade individual, ciclo de vida controlado e autenticação proporcional ao risco.

- Inventariar contas de usuário, administrador e serviço; validar contas ativas ao menos trimestralmente.
- Exigir MFA para acesso remoto, nuvem, e-mail, administrativo e sistemas críticos, quando tecnicamente possível.
- Proibir compartilhamento de senha; armazenar segredo em cofre e proteger contra força bruta.

4.4 Concessão, revisão e revogação de acessos

Acesso segue aprovação do proprietário, menor privilégio, segregação e necessidade de conhecer.

- Integrar admissão, mudança e desligamento; revogar imediatamente em desligamentos de risco.
- Revisar acessos privilegiados e críticos trimestralmente e demais acessos em ciclo definido.
- Registrar solicitação, aprovação, execução, revisão e exceção.

4.5 Configuração segura, hardening e mudanças

Ativos e software devem seguir baselines aprovadas, com serviços mínimos, configuração rastreável e mudança controlada.

- Revisar baselines ao menos anualmente e quando houver ameaça ou versão relevante.
- Segregar desenvolvimento, homologação e produção quando houver desenvolvimento ou configuração aplicável.
- Testar, aprovar, registrar, possuir rollback e realizar revisão pós-implementação.

4.6 Endpoints, mobilidade e trabalho remoto

Dispositivos autorizados devem usar criptografia, bloqueio, atualização, proteção antimalware/EDR e capacidade de gestão compatível.

- Evitar armazenamento local; usar repositórios corporativos e VPN/acesso seguro quando requerido.
- Proteger tela, voz, papel e equipamento em local público ou compartilhado.
- Comunicar perda, furto, suspeita de comprometimento ou viagem de risco imediatamente.

4.7 Rede, e-mail, web e malware

A infraestrutura deve ser segmentada, atualizada e monitorada, com proteção de navegação, correio, DNS e malware.

- Manter versões suportadas e revisar software de rede mensalmente.
- Aplicar filtros de phishing, anexos, links e execução; testar conscientização de forma ética.
- Centralizar alertas relevantes e definir resposta a detecção.

4.8 Criptografia e gestão de chaves

Criptografia deve proteger dados em trânsito e em repouso conforme classificação e risco.

- Utilizar HTTPS/TLS atual e protocolos aprovados; desabilitar versões inseguras.
- Gerir criação, armazenamento, rotação, backup, revogação e acesso a chaves e certificados.
- Não confundir criptografia com anonimização; preservar capacidade de restauração autorizada.

4.9 Logs, auditoria e monitoramento

Eventos relevantes devem registrar data/hora sincronizada, identidade, ação, ativo, origem, resultado e alteração, sem coletar conteúdo excessivo.

- Definir fontes, retenção, proteção contra alteração, revisão, alertas e responsáveis.
- Centralizar e correlacionar logs críticos em SIEM ou capacidade equivalente proporcional.
- Restringir logs que contenham dados pessoais ou sigilo e testar alertas.

4.10 Vulnerabilidades, patches e inteligência de ameaças

A VGF mantém processo documentado para identificar, analisar, priorizar, tratar e verificar vulnerabilidades.

- Inventariar exposição, executar varreduras proporcionais e acompanhar avisos de fornecedores.
- Definir SLA por criticidade e aceitar exceção somente com risco e controle compensatório aprovados.
- Realizar reteste e preservar evidência de correção.

4.11 Desenvolvimento, aquisição e aplicações seguras

Aplicações desenvolvidas, configuradas ou adquiridas devem incorporar segurança no ciclo de vida.

- Definir requisitos, modelagem de ameaça, revisão, SAST/DAST/SCA quando aplicável e aprovação antes de produção.

- Seguir OWASP para web e API, prevenindo injeção, XSS, falhas de autenticação, autorização e segredo.
- Controlar dependências, código de terceiros, ambientes, versões e documentação técnica/funcional.

4.12 Nuvem e responsabilidade compartilhada

Serviços de nuvem são aprovados após avaliação de dados, localização, arquitetura, segurança, continuidade, suboperadores, saída e responsabilidade entre VGF e provedor.

- Manter inventário de SaaS e impedir shadow IT.
- Configurar identidade, MFA, logs, criptografia, backup, segregação de tenants e alertas conforme risco.
- Verificar SLA, regiões, suporte, portabilidade, eliminação, incidentes, auditoria e certificações do provedor sem atribuí-las à VGF.

4.13 Arquitetura, integrações e requisitos de solução

Requisitos como SaaS, browser, Entra ID, SSO, OAuth2, JWT, API REST, WS-Security, exportação, idioma, personalização, segregação, multi-cloud e responsividade devem ser avaliados caso a caso.

- Registrar Atende, Atende Parcialmente, Não Atende ou Não se Aplica com justificativa e evidência.
- Não assumir capacidade por existir nesta Política; validar por teste, documento do produto, contrato ou demonstração.
- Tratar requisito eliminatório e dependência de terceiro antes de compromisso comercial.

IMPORTANTE A matriz do formulário contém requisitos de produto que podem não se aplicar a serviços jurídicos. A resposta correta deve refletir o objeto contratado e a solução efetivamente oferecida.

4.14 Backup, recuperação e continuidade

Dados e configurações críticas devem possuir backup protegido, retenção, cópia segregada e teste de restauração.

- Definir RTO, RPO, prioridade, dependências, responsáveis e comunicação.
- Criptografar backup, restringir acesso e considerar cópia imutável/offline conforme risco.
- Testar restauração e plano de continuidade ao menos anualmente e após mudança relevante.

4.15 Gestão de incidentes cibernéticos

A VGF mantém capacidade para preparar, detectar, analisar, conter, erradicar, recuperar, comunicar e aprender.

- Designar titular e substituto, contatos, severidade, playbooks, cadeia de custódia e critérios de escalonamento.
- Preservar privilégio e sigilo na investigação, sem impedir obrigações de comunicação.
- Integrar Segurança, DPO, Jurídico, Comunicação, Pessoas, fornecedores e liderança.

4.16 Fornecedores e cadeia de tecnologia

Provedores que mantêm dados sensíveis ou suportam processos críticos devem ser inventariados, classificados, avaliados e monitorados.

- Definir contato interno, serviço, dados, criticidade, regiões, subcontratados, SLA, saída e risco.
- Exigir segurança, privacidade, incidente, continuidade, auditoria e devolução/eliminação em contrato.
- Revisar anualmente ou por mudança significativa.

4.17 Testes de segurança e invasão

Programa de testes deve ser proporcional a exposição, complexidade, mudança e criticidade.

- Definir escopo, método, frequência, regras de engajamento, qualificação, proteção de dados e responsáveis.
- Abranger rede, aplicações, APIs, nuvem e engenharia social quando autorizada.
- Rastrear achados, prioridade, remediação, aceitação e reteste.

4.18 Uso aceitável, colaboração e inteligência artificial

Recursos corporativos destinam-se a fins autorizados. É vedado contornar controles, instalar software sem aprovação, compartilhar credencial ou inserir informação restrita em serviço não aprovado.

- Aplicar rotulagem e destinatário correto antes de enviar; confirmar links e solicitações financeiras.
- Usar IA somente em ambiente e caso aprovados, com revisão humana e proteção de segredo.
- Respeitar direitos autorais, licenças, privacidade, ética e registro profissional.

4.19 Descarte e sanitização

Ativos, papel e mídia devem ser sanitizados conforme risco antes de reutilização, devolução ou descarte.

- Usar exclusão criptográfica, sobrescrita, destruição física ou método equivalente verificado.
- Manter cadeia de custódia e certificado para terceiro relevante.
- Remover contas, chaves, tokens, perfis e cópias associadas.

5. Governança, aplicação, monitoramento e rastreabilidade

5.1 Comunicação, educação e aceite

A VGF disponibiliza conteúdo, trilhas de aprendizagem e assinatura eletrônica de termos na Academy Volk (https://academyvolk.ultramidnal.com.br/), sem prejuízo de orientações presenciais ou em outros canais oficiais.

- Capacitação no ingresso e reciclagem ao menos anual, com módulos proporcionais à função e ao risco.
- Registro de convocação, participação, conclusão, avaliação de aprendizagem e aceite da versão vigente.
- Conteúdo extraordinário quando houver incidente, alteração relevante, nova tecnologia, serviço ou requisito.

5.2 Canal, consulta, relato e não retaliação

Dúvidas e relatos podem ser encaminhados à liderança competente ou à Ouvidoria (ouvidoria@vgfadv.com.br). Questões de dados pessoais devem ser dirigidas aos canais do DPO (lgpd@vgfadv.com.br | sancle.albuquerque@midnal.com.br).

- Relatos de boa-fé devem ser recebidos com respeito, confidencialidade, independência e proibição de retaliação.
- A identidade será restrita ao necessário; anonimato será preservado quando oferecido e juridicamente possível.
- Urgências de segurança, integridade física, fraude ou destruição de evidências exigem escalonamento imediato.

5.3 Monitoramento, desvios e melhoria contínua

A efetividade é monitorada por indicadores, testes amostrais, avaliações de risco, reclamações, incidentes, auditorias, diligências e análise crítica da liderança.

- Não conformidades devem ser registradas, contidas, analisadas quanto à causa e tratadas com responsável e prazo.
- Medidas disciplinares são proporcionais, coerentes, documentadas e aplicadas com contraditório quando cabível.
- Resultados relevantes alimentam revisão de riscos, controles, treinamento e documentação.

5.4 Gestão documental e exceções

Somente documentos aprovados e vigentes podem orientar a operação. Exceções devem ser raras, justificadas, temporárias, avaliadas quanto ao risco e aprovadas por autoridade competente.

- Preservar autoria, aprovação, versão, data, classificação, local oficial e prazo de revisão.
- Retirar ou identificar cópias obsoletas e impedir uso não intencional.
- Registrar aceite de risco, controles compensatórios, responsável e data de expiração da exceção.

5.5 ISO/IEC 27001:2022 — cláusulas do SGSI

Cobertura das cláusulas 4 a 10 do sistema de gestão de segurança da informação.

USO DA MATRIZ Os identificadores facilitam rastreabilidade e auditoria. As descrições são sínteses executivas e não substituem a aquisição, leitura e interpretação da norma oficial aplicável.

Referência	Controle / requisito	Aplicação executiva na VGF	Evidências e verificação
Cl. 4	Contexto da organização	Definir escopo do SGSI, partes interessadas, requisitos e interfaces relevantes para segurança da informação, cibersegurança e nuvem.	Escopo aprovado, mapa de partes interessadas, requisitos e processos.
Cl. 5	Liderança	Demonstrar compromisso, aprovar política, atribuir papéis e integrar segurança da informação, cibersegurança e nuvem às decisões da VGF.	Política, organograma, atas, comunicações e provisão de recursos.
Cl. 6	Planejamento	Avaliar riscos e oportunidades, definir objetivos mensuráveis e planejar mudanças relacionadas a segurança da informação, cibersegurança e nuvem.	Matriz de riscos, objetivos, indicadores, planos e aceites de risco.
Cl. 7	Apoio	Assegurar recursos, competência, conscientização, comunicação e informação documentada controlada.	Orçamento, competências, Academy, comunicações e controle documental.
Cl. 8	Operação	Planejar, executar e controlar processos e terceiros que materializam segurança da informação, cibersegurança e nuvem, inclusive mudanças e exceções.	Procedimentos, contratos, tickets, aprovações, testes e registros operacionais.
Cl. 9	Avaliação de desempenho	Monitorar indicadores, realizar auditoria interna proporcional e promover análise crítica da liderança.	Dashboards, testes, auditorias, atas e planos de correção.

Cl. 10	Melhoria	Tratar não conformidades e incidentes, eliminar causas, verificar eficácia e melhorar continuamente.	Registro de desvios, causa raiz, ações, verificação e lições aprendidas.

5.6 ISO/IEC 27001:2022 — catálogo dos 93 controles do Anexo A

Cobertura individual, parafraseada e vinculada aos capítulos internos, dos 37 controles organizacionais, 8 de pessoas, 14 físicos e 34 tecnológicos.

USO DA MATRIZ Os identificadores facilitam rastreabilidade e auditoria. As descrições são sínteses executivas e não substituem a aquisição, leitura e interpretação da norma oficial aplicável.

Referência	Controle / requisito	Aplicação executiva na VGF	Evidências e verificação
A.5.1	Organizacionais — Políticas de segurança	Aplicar por processo documentado e baseado em risco, com proprietário, frequência, exceção aprovada e vínculo aos capítulos 4.1; 5.4.	Políticas aprovadas, versões, divulgação e revisão.
A.5.2	Organizacionais — Papéis e responsabilidades	Aplicar por processo documentado e baseado em risco, com proprietário, frequência, exceção aprovada e vínculo aos capítulos 3.2; 4.15.	RACI, designações, substitutos e atas.
A.5.3	Organizacionais — Segregação de funções	Aplicar por processo documentado e baseado em risco, com proprietário, frequência, exceção aprovada e vínculo aos capítulos 4.4–4.5.	Matriz de alçadas, perfis e testes de conflito.
A.5.4	Organizacionais — Responsabilidades da gestão	Aplicar por processo documentado e baseado em risco, com proprietário, frequência, exceção aprovada e vínculo aos capítulos 3.2; 5.1.	Comunicações, avaliações e ações de gestores.
A.5.5	Organizacionais — Contato com autoridades	Aplicar por processo documentado e baseado em risco, com proprietário, frequência, exceção aprovada e vínculo aos capítulos 4.15; 5.2.	Lista de contatos, critérios e registros de comunicação.
A.5.6	Organizacionais — Grupos especializados	Aplicar por processo documentado e baseado em risco, com proprietário, frequência, exceção aprovada e vínculo aos capítulos 4.10; 5.3.	Associações, alertas recebidos e ações correlatas.
A.5.7	Organizacionais — Inteligência de ameaças	Aplicar por processo documentado e baseado em risco, com proprietário, frequência, exceção aprovada e vínculo aos capítulos 4.10.	Fontes, boletins, triagem, impacto e tratamento.
A.5.8	Organizacionais — Segurança em projetos	Aplicar por processo documentado e baseado em risco, com proprietário, frequência, exceção aprovada e vínculo aos capítulos 4.11–4.13.	Gate de segurança, requisitos, riscos e aceite.
A.5.9	Organizacionais — Inventário de ativos e informação	Aplicar por processo documentado e baseado em risco, com proprietário, frequência, exceção aprovada e vínculo aos capítulos 4.1.	CMDB, inventários, proprietário e revisão.
A.5.10	Organizacionais — Uso aceitável	Aplicar por processo documentado e baseado em risco, com proprietário, frequência, exceção aprovada e vínculo aos capítulos 4.18.	Termos, regras, treinamento e monitoramento proporcional.
A.5.11	Organizacionais — Devolução de ativos	Aplicar por processo documentado e baseado em risco, com proprietário, frequência, exceção aprovada e vínculo aos capítulos 4.6; 4.19.	Checklist de desligamento, baixa e comprovante.
A.5.12	Organizacionais — Classificação da informação	Aplicar por processo documentado e baseado em risco, com proprietário, frequência, exceção aprovada e vínculo aos capítulos 4.2.	Esquema de classificação, inventário e amostras.
A.5.13	Organizacionais — Rotulagem da informação	Aplicar por processo documentado e baseado em risco, com proprietário, frequência, exceção aprovada e vínculo aos capítulos 4.2.	Rótulos, metadados, templates e testes.
A.5.14	Organizacionais — Transferência de informação	Aplicar por processo documentado e baseado em risco, com proprietário, frequência, exceção aprovada e vínculo aos capítulos 4.2; 4.8.	Regras de envio, criptografia, DLP e contratos.
A.5.15	Organizacionais — Controle de acesso	Aplicar por processo documentado e baseado em risco, com proprietário, frequência, exceção aprovada e vínculo aos capítulos 4.3–4.4.	Política, matriz, regras e revisões.

A.5.16	Organizacionais — Gestão de identidades	Aplicar por processo documentado e baseado em risco, com proprietário, frequência, exceção aprovada e vínculo aos capítulos 4.3.	Cadastro, JML, contas de serviço e reconciliação.
A.5.17	Organizacionais — Informações de autenticação	Aplicar por processo documentado e baseado em risco, com proprietário, frequência, exceção aprovada e vínculo aos capítulos 4.3; 4.8.	MFA, cofre, rotação, recuperação e logs.
A.5.18	Organizacionais — Direitos de acesso	Aplicar por processo documentado e baseado em risco, com proprietário, frequência, exceção aprovada e vínculo aos capítulos 4.4.	Solicitações, aprovações, recertificação e revogação.
A.5.19	Organizacionais — Segurança em relações com fornecedores	Aplicar por processo documentado e baseado em risco, com proprietário, frequência, exceção aprovada e vínculo aos capítulos 4.16.	Inventário, classificação, risco e diligência.
A.5.20	Organizacionais — Segurança em acordos com fornecedores	Aplicar por processo documentado e baseado em risco, com proprietário, frequência, exceção aprovada e vínculo aos capítulos 4.16.	Cláusulas, SLA, auditoria, incidentes e saída.
A.5.21	Organizacionais — Cadeia de suprimentos de TIC	Aplicar por processo documentado e baseado em risco, com proprietário, frequência, exceção aprovada e vínculo aos capítulos 4.11; 4.16.	Origem, dependências, SBOM/SCA quando cabível e risco.
A.5.22	Organizacionais — Monitoramento e mudanças de fornecedores	Aplicar por processo documentado e baseado em risco, com proprietário, frequência, exceção aprovada e vínculo aos capítulos 4.16.	Revisões, atestados, ocorrências, mudanças e ações.
A.5.23	Organizacionais — Uso de serviços em nuvem	Aplicar por processo documentado e baseado em risco, com proprietário, frequência, exceção aprovada e vínculo aos capítulos 4.12–4.13.	Avaliação cloud, regiões, configuração, SLA e saída.
A.5.24	Organizacionais — Preparação para incidentes	Aplicar por processo documentado e baseado em risco, com proprietário, frequência, exceção aprovada e vínculo aos capítulos 4.15.	Plano, RACI, playbooks, contatos e exercícios.
A.5.25	Organizacionais — Avaliação de eventos	Aplicar por processo documentado e baseado em risco, com proprietário, frequência, exceção aprovada e vínculo aos capítulos 4.15.	Critérios, severidade, triagem e decisão registrada.
A.5.26	Organizacionais — Resposta a incidentes	Aplicar por processo documentado e baseado em risco, com proprietário, frequência, exceção aprovada e vínculo aos capítulos 4.15.	Tickets, contenção, comunicação, recuperação e decisão.
A.5.27	Organizacionais — Aprendizado com incidentes	Aplicar por processo documentado e baseado em risco, com proprietário, frequência, exceção aprovada e vínculo aos capítulos 4.15; 5.3.	Causa raiz, retrospectiva e atualização de controles.
A.5.28	Organizacionais — Coleta de evidências	Aplicar por processo documentado e baseado em risco, com proprietário, frequência, exceção aprovada e vínculo aos capítulos 4.15.	Cadeia de custódia, hashes, autoridade e preservação.
A.5.29	Organizacionais — Segurança durante interrupções	Aplicar por processo documentado e baseado em risco, com proprietário, frequência, exceção aprovada e vínculo aos capítulos 4.14–4.15.	BCP, controles mínimos e registros de crise.
A.5.30	Organizacionais — Prontidão de TIC para continuidade	Aplicar por processo documentado e baseado em risco, com proprietário, frequência, exceção aprovada e vínculo aos capítulos 4.14.	BIA, RTO/RPO, redundância e testes.
A.5.31	Organizacionais — Requisitos legais e contratuais	Aplicar por processo documentado e baseado em risco, com proprietário, frequência, exceção aprovada e vínculo aos capítulos 2; 4.2; 5.5.	Cadastro de requisitos, contratos e avaliação.
A.5.32	Organizacionais — Direitos de propriedade intelectual	Aplicar por processo documentado e baseado em risco, com proprietário, frequência, exceção aprovada e vínculo aos capítulos 4.11; 4.18.	Licenças, termos, inventário e verificações.
A.5.33	Organizacionais — Proteção de registros	Aplicar por processo documentado e baseado em risco, com proprietário, frequência, exceção aprovada e vínculo aos capítulos 4.2; 4.9; seção 6.	Tabela de retenção, imutabilidade e descarte.
A.5.34	Organizacionais — Privacidade e dados pessoais	Aplicar por processo documentado e baseado em risco, com proprietário, frequência, exceção aprovada e vínculo aos capítulos 4.2; 4.12; 5.5.	ROPA, RIPD, DPA, direitos e controles.
A.5.35	Organizacionais — Revisão independente	Aplicar por processo documentado e baseado em risco, com proprietário, frequência, exceção aprovada e vínculo aos capítulos 5.3.	Auditoria, escopo, independência, achados e ações.

A.5.36	Organizacionais — Conformidade com regras de segurança	Aplicar por processo documentado e baseado em risco, com proprietário, frequência, exceção aprovada e vínculo aos capítulos 5.3–5.4.	Testes, exceções, métricas e planos.
A.5.37	Organizacionais — Procedimentos operacionais documentados	Aplicar por processo documentado e baseado em risco, com proprietário, frequência, exceção aprovada e vínculo aos capítulos 4; 5.4.	Procedimentos, versões, acesso e evidências de uso.
A.6.1	Pessoas — Verificação prévia	Aplicar por processo documentado e baseado em risco, com proprietário, frequência, exceção aprovada e vínculo aos capítulos 3.2; 4.16.	Critérios, consentimentos, registros e decisão.
A.6.2	Pessoas — Termos e condições de vínculo	Aplicar por processo documentado e baseado em risco, com proprietário, frequência, exceção aprovada e vínculo aos capítulos 4.18; 5.1.	Contrato, NDA, deveres e aceite.
A.6.3	Pessoas — Conscientização e treinamento	Aplicar por processo documentado e baseado em risco, com proprietário, frequência, exceção aprovada e vínculo aos capítulos 5.1.	Programa, Academy, avaliação e métricas.
A.6.4	Pessoas — Processo disciplinar	Aplicar por processo documentado e baseado em risco, com proprietário, frequência, exceção aprovada e vínculo aos capítulos 5.2–5.3.	Regras, apuração, decisão e proporcionalidade.
A.6.5	Pessoas — Responsabilidades após mudança ou término	Aplicar por processo documentado e baseado em risco, com proprietário, frequência, exceção aprovada e vínculo aos capítulos 4.4; 4.19.	Revogação, devolução, transição e lembrete.
A.6.6	Pessoas — Confidencialidade	Aplicar por processo documentado e baseado em risco, com proprietário, frequência, exceção aprovada e vínculo aos capítulos 4.2; 4.18.	NDA, cláusulas, treinamento e incidentes.
A.6.7	Pessoas — Trabalho remoto	Aplicar por processo documentado e baseado em risco, com proprietário, frequência, exceção aprovada e vínculo aos capítulos 4.6.	Padrão remoto, configuração, inspeção e aceite.
A.6.8	Pessoas — Comunicação de eventos	Aplicar por processo documentado e baseado em risco, com proprietário, frequência, exceção aprovada e vínculo aos capítulos 4.15; 5.2.	Canais, registros, tempos e resposta.
A.7.1	Físicos — Perímetros físicos	Aplicar por processo documentado e baseado em risco, com proprietário, frequência, exceção aprovada e vínculo aos capítulos 4.2; 4.6.	Planta, barreiras, revisão e ocorrências.
A.7.2	Físicos — Entrada física	Aplicar por processo documentado e baseado em risco, com proprietário, frequência, exceção aprovada e vínculo aos capítulos 4.2; 4.6.	Crachás, visitantes, logs e revogação.
A.7.3	Físicos — Proteção de escritórios e salas	Aplicar por processo documentado e baseado em risco, com proprietário, frequência, exceção aprovada e vínculo aos capítulos 4.2; 4.6.	Fechaduras, zonas, regras e inspeções.
A.7.4	Físicos — Monitoramento físico	Aplicar por processo documentado e baseado em risco, com proprietário, frequência, exceção aprovada e vínculo aos capítulos 4.2; 5.5.	CFTV/alertas, retenção, aviso e revisão.
A.7.5	Físicos — Ameaças físicas e ambientais	Aplicar por processo documentado e baseado em risco, com proprietário, frequência, exceção aprovada e vínculo aos capítulos 4.14.	Avaliação, sensores, seguros e continuidade.
A.7.6	Físicos — Trabalho em áreas seguras	Aplicar por processo documentado e baseado em risco, com proprietário, frequência, exceção aprovada e vínculo aos capítulos 4.2; 4.6.	Autorizações, acompanhantes e logs.
A.7.7	Físicos — Mesa e tela limpas	Aplicar por processo documentado e baseado em risco, com proprietário, frequência, exceção aprovada e vínculo aos capítulos 4.2; 4.6.	Regras, inspeções e conscientização.
A.7.8	Físicos — Posicionamento e proteção de equipamentos	Aplicar por processo documentado e baseado em risco, com proprietário, frequência, exceção aprovada e vínculo aos capítulos 4.6.	Checklist, inventário e inspeção.
A.7.9	Físicos — Ativos fora das instalações	Aplicar por processo documentado e baseado em risco, com proprietário, frequência, exceção aprovada e vínculo aos capítulos 4.6.	Autorização, criptografia, rastreio e ocorrência.
A.7.10	Físicos — Mídias de armazenamento	Aplicar por processo documentado e baseado em risco, com proprietário, frequência, exceção aprovada e vínculo aos capítulos 4.2; 4.19.	Inventário, criptografia, custódia e descarte.

A.7.11	Físicos — Utilidades de suporte	Aplicar por processo documentado e baseado em risco, com proprietário, frequência, exceção aprovada e vínculo aos capítulos 4.14.	UPS, energia, climatização, manutenção e testes.
A.7.12	Físicos — Segurança de cabeamento	Aplicar por processo documentado e baseado em risco, com proprietário, frequência, exceção aprovada e vínculo aos capítulos 4.7.	Plantas, proteção, inspeção e mudanças.
A.7.13	Físicos — Manutenção de equipamentos	Aplicar por processo documentado e baseado em risco, com proprietário, frequência, exceção aprovada e vínculo aos capítulos 4.1; 4.5.	Agenda, fornecedor, autorização e registro.
A.7.14	Físicos — Descarte ou reutilização segura	Aplicar por processo documentado e baseado em risco, com proprietário, frequência, exceção aprovada e vínculo aos capítulos 4.19.	Sanitização, certificado, baixa e cadeia de custódia.
A.8.1	Tecnológicos — Dispositivos de usuário	Aplicar por processo documentado e baseado em risco, com proprietário, frequência, exceção aprovada e vínculo aos capítulos 4.6.	MDM/gestão, criptografia, EDR, patches e inventário.
A.8.2	Tecnológicos — Acessos privilegiados	Aplicar por processo documentado e baseado em risco, com proprietário, frequência, exceção aprovada e vínculo aos capítulos 4.3–4.4.	PAM/cofre, contas nominativas, logs e revisão.
A.8.3	Tecnológicos — Restrição de acesso à informação	Aplicar por processo documentado e baseado em risco, com proprietário, frequência, exceção aprovada e vínculo aos capítulos 4.2; 4.4.	ACL, grupos, barreiras éticas e testes.
A.8.4	Tecnológicos — Acesso a código-fonte	Aplicar por processo documentado e baseado em risco, com proprietário, frequência, exceção aprovada e vínculo aos capítulos 4.11.	Repositório, MFA, branches, revisão e logs.
A.8.5	Tecnológicos — Autenticação segura	Aplicar por processo documentado e baseado em risco, com proprietário, frequência, exceção aprovada e vínculo aos capítulos 4.3.	MFA, políticas, testes e telemetria.
A.8.6	Tecnológicos — Gestão de capacidade	Aplicar por processo documentado e baseado em risco, com proprietário, frequência, exceção aprovada e vínculo aos capítulos 4.9; 4.14.	Métricas, limites, previsão e alertas.
A.8.7	Tecnológicos — Proteção contra malware	Aplicar por processo documentado e baseado em risco, com proprietário, frequência, exceção aprovada e vínculo aos capítulos 4.7.	EDR/antimalware, políticas, cobertura e incidentes.
A.8.8	Tecnológicos — Vulnerabilidades técnicas	Aplicar por processo documentado e baseado em risco, com proprietário, frequência, exceção aprovada e vínculo aos capítulos 4.10.	Scans, SLA, tickets, exceções e reteste.
A.8.9	Tecnológicos — Gestão de configuração	Aplicar por processo documentado e baseado em risco, com proprietário, frequência, exceção aprovada e vínculo aos capítulos 4.5.	Baselines, inventário, conformidade e mudanças.
A.8.10	Tecnológicos — Exclusão de informação	Aplicar por processo documentado e baseado em risco, com proprietário, frequência, exceção aprovada e vínculo aos capítulos 4.19.	Regras, logs, verificação e certificados.
A.8.11	Tecnológicos — Mascaramento de dados	Aplicar por processo documentado e baseado em risco, com proprietário, frequência, exceção aprovada e vínculo aos capítulos 4.2; 4.11.	Regras, ambientes, testes e aprovação.
A.8.12	Tecnológicos — Prevenção de vazamento	Aplicar por processo documentado e baseado em risco, com proprietário, frequência, exceção aprovada e vínculo aos capítulos 4.2; 4.9.	DLP, regras, alertas, exceções e incidentes.
A.8.13	Tecnológicos — Backup	Aplicar por processo documentado e baseado em risco, com proprietário, frequência, exceção aprovada e vínculo aos capítulos 4.14.	Escopo, retenção, criptografia e restauração.
A.8.14	Tecnológicos — Redundância	Aplicar por processo documentado e baseado em risco, com proprietário, frequência, exceção aprovada e vínculo aos capítulos 4.14.	Arquitetura, capacidade, failover e teste.
A.8.15	Tecnológicos — Registro de eventos	Aplicar por processo documentado e baseado em risco, com proprietário, frequência, exceção aprovada e vínculo aos capítulos 4.9.	Fontes, campos, retenção, integridade e acesso.
A.8.16	Tecnológicos — Monitoramento de atividades	Aplicar por processo documentado e baseado em risco, com proprietário, frequência, exceção aprovada e vínculo aos capítulos 4.9.	Casos de uso, alertas, triagem e métricas.

A.8.17	Tecnológicos — Sincronização de relógios	Aplicar por processo documentado e baseado em risco, com proprietário, frequência, exceção aprovada e vínculo aos capítulos 4.9.	NTP, configuração, desvio e verificação.
A.8.18	Tecnológicos — Utilitários privilegiados	Aplicar por processo documentado e baseado em risco, com proprietário, frequência, exceção aprovada e vínculo aos capítulos 4.3–4.5.	Lista permitida, execução, logs e revisão.
A.8.19	Tecnológicos — Instalação de software em produção	Aplicar por processo documentado e baseado em risco, com proprietário, frequência, exceção aprovada e vínculo aos capítulos 4.5; 4.11.	Aprovação, pacote, teste, versão e rollback.
A.8.20	Tecnológicos — Segurança de redes	Aplicar por processo documentado e baseado em risco, com proprietário, frequência, exceção aprovada e vínculo aos capítulos 4.7.	Arquitetura, regras, patches, testes e monitoramento.
A.8.21	Tecnológicos — Segurança de serviços de rede	Aplicar por processo documentado e baseado em risco, com proprietário, frequência, exceção aprovada e vínculo aos capítulos 4.7; 4.16.	Requisitos, SLA, criptografia e relatórios.
A.8.22	Tecnológicos — Segregação de redes	Aplicar por processo documentado e baseado em risco, com proprietário, frequência, exceção aprovada e vínculo aos capítulos 4.7; 4.12.	VLAN/segmentação, regras, diagrama e teste.
A.8.23	Tecnológicos — Filtragem web	Aplicar por processo documentado e baseado em risco, com proprietário, frequência, exceção aprovada e vínculo aos capítulos 4.7.	Política, categorias, logs, exceções e métricas.
A.8.24	Tecnológicos — Criptografia	Aplicar por processo documentado e baseado em risco, com proprietário, frequência, exceção aprovada e vínculo aos capítulos 4.8.	Padrões, chaves, certificados, rotação e testes.
A.8.25	Tecnológicos — Ciclo de desenvolvimento seguro	Aplicar por processo documentado e baseado em risco, com proprietário, frequência, exceção aprovada e vínculo aos capítulos 4.11.	SDLC, gates, papéis, treinamento e métricas.
A.8.26	Tecnológicos — Requisitos de segurança de aplicações	Aplicar por processo documentado e baseado em risco, com proprietário, frequência, exceção aprovada e vínculo aos capítulos 4.11–4.13.	Requisitos, histórias, critérios e aceite.
A.8.27	Tecnológicos — Arquitetura e engenharia seguras	Aplicar por processo documentado e baseado em risco, com proprietário, frequência, exceção aprovada e vínculo aos capítulos 4.11–4.13.	Princípios, threat model, revisão e decisão.
A.8.28	Tecnológicos — Codificação segura	Aplicar por processo documentado e baseado em risco, com proprietário, frequência, exceção aprovada e vínculo aos capítulos 4.11.	Padrões, revisão, SAST e capacitação.
A.8.29	Tecnológicos — Testes de segurança	Aplicar por processo documentado e baseado em risco, com proprietário, frequência, exceção aprovada e vínculo aos capítulos 4.11; 4.17.	Plano, SAST/DAST/SCA, pentest e reteste.
A.8.30	Tecnológicos — Desenvolvimento terceirizado	Aplicar por processo documentado e baseado em risco, com proprietário, frequência, exceção aprovada e vínculo aos capítulos 4.11; 4.16.	Contrato, código, testes, propriedade e aceite.
A.8.31	Tecnológicos — Separação de ambientes	Aplicar por processo documentado e baseado em risco, com proprietário, frequência, exceção aprovada e vínculo aos capítulos 4.5; 4.11.	Inventário, acessos, dados e evidência de segregação.
A.8.32	Tecnológicos — Gestão de mudanças	Aplicar por processo documentado e baseado em risco, com proprietário, frequência, exceção aprovada e vínculo aos capítulos 4.5.	Ticket, risco, teste, aprovação e rollback.
A.8.33	Tecnológicos — Informações de teste	Aplicar por processo documentado e baseado em risco, com proprietário, frequência, exceção aprovada e vínculo aos capítulos 4.11.	Mascaramento, autorização, retenção e exclusão.
A.8.34	Tecnológicos — Proteção durante testes de auditoria	Aplicar por processo documentado e baseado em risco, com proprietário, frequência, exceção aprovada e vínculo aos capítulos 4.17; 5.3.	Escopo, janela, autorização, backup e acompanhamento.

5.7 Referências normativas e informacionais

As referências abaixo orientam a interpretação e a atualização deste documento. Normas técnicas são aplicadas de forma proporcional ao contexto da VGF e não representam declaração de certificação.

- Portal institucional da VGF Advogados — https://www.vgfadv.com.br
- Código de Ética e Disciplina da OAB — https://www.oab.org.br/leisnormas/legislacao/resolucoes/02-2015
- Provimento CFOAB nº 205/2021 — publicidade e informação da advocacia — https://www.oab.org.br/leisnormas/legislacao/provimentos/205-2021
- ISO/IEC 27001:2022 — SGSI — https://www.iso.org/standard/27001
- Lei nº 13.709/2018 — LGPD — https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709compilado.htm
- ANPD — Comunicação de incidente de segurança — https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/comunicado-de-incidente-de-seguranca-cis
- OWASP Top 10 — https://owasp.org/www-project-top-ten/
- CIS Controls v8 — https://www.cisecurity.org/controls/v8

5.8 Matriz de rastreabilidade para avaliações de terceiros

A matriz indica onde o compromisso está definido e qual evidência operacional deve corroborar eventual resposta a questionários. A política, isoladamente, demonstra desenho de controle; a efetividade depende de registros atuais, amostras, configurações, contratos, relatórios ou entrevistas.

Formulário / item	Tema avaliado	Referência neste documento	Evidência recomendada
Maturidade 1.1–3.1	Ativos, software e gestão/classificação de dados.	4.1–4.2	Inventários, proprietários, revisões, classificação, retenção e descarte.
Maturidade 4.1–6.1	Configuração, contas e acessos.	4.3–4.5	Baselines, inventário de contas, JML, aprovações e revisões.
Maturidade 7.1–10.1	Vulnerabilidades, logs, e-mail/web e antimalware.	4.7; 4.9–4.10	Scans, patches, SIEM/logs, filtros, EDR e testes.
Maturidade 11.1–13.1	Recuperação, rede e monitoramento.	4.7; 4.14	Política de backup, testes, inventário de rede, versões e alertas.
Maturidade 14.1–15.1	Conscientização e provedores.	4.16; 4.18; 5.1	Academy, avaliações, inventário, classificação e diligência.
Maturidade 16.1–18.1	SDLC, incidentes e pentest.	4.11; 4.15; 4.17	SDLC, SAST/DAST/SCA, RACI, playbooks, relatórios e retestes.
Arquitetura 1–12	SaaS, browser, HTTPS, identidade, exportação, idioma, visual e perfis.	4.3–4.4; 4.8; 4.12–4.13	Ficha técnica, demo/teste, arquitetura, contrato e matriz de acessos.
Arquitetura 13–22	Logs, LGPD, CIA, segregação, data center, certificações, TLS, multi-cloud, monitoramento e backup.	4.2; 4.8–4.9; 4.12; 4.14	Logs, DPA, desenho de tenant, SLA, atestados do provedor, monitoramento e restore.
Arquitetura 23–36	Versão, documentação, mudanças, ambientes, OWASP, mobile, suporte, APIs e testes.	4.5; 4.11; 4.13; 4.17	Release notes, manuais, change tickets, testes, SLA, especificação de API e pentest.

5.C01 Caderno de controle — governança do SGSI, escopo e apetite a risco

LEITURA EXECUTIVA Este caderno converte o compromisso sobre governança do sgsi, escopo e apetite a risco em uma rotina verificável. Aplica-se a informações, pessoas, equipamentos, aplicações, redes, instalações, serviços em nuvem, fornecedores e ambientes de trabalho remoto e deve ser usado antes da decisão, durante a execução e na revisão de eficácia. O objetivo é permitir que qualquer leitor compreenda o que deve ser feito, quem decide, qual evidência comprova a prática e quando o tema precisa ser escalado.

Objetivo, resultado e critério de aceitação

O resultado esperado para governança do sgsi, escopo e apetite a risco é uma decisão coerente com confidencialidade, integridade, disponibilidade, autenticidade, rastreabilidade, ISO/IEC 27001:2022 e controles do Anexo A, baseada em risco, documentada no nível proporcional ao impacto e passível de reconstrução por terceiro independente. O controle é considerado implementado somente quando há responsável designado, critério prévio, execução demonstrável, tratamento de exceções e verificação periódica.

Aplicação operacional mínima

- Planejar: o Segurança da Informação e proprietário do ativo ou serviço define finalidade, entradas, critérios, alçada, prazo e evidência necessária para governança do sgsi, escopo e apetite a risco.
- Executar: utilizar fluxo oficial, segregação de funções e validações proporcionais; decisões sensíveis dependem de responsável pelo SGSI, Comitê multidisciplinar ou Diretoria para risco residual alto.
- Registrar: preservar solicitação, análise, aprovação, resultado, comunicação e eventual exceção em ferramentas oficiais de gestão de ativos, identidade, tickets, logs, monitoramento e riscos.
- Verificar: realizar contínua para eventos; mensal, trimestral ou anual conforme criticidade; e após mudança ou incidente teste de desenho e amostra de eficácia, registrando população, seleção, resultado e conclusão.
- Corrigir: desvios devem ser contidos, avaliados quanto à causa, tratados por plano com responsável e submetidos a reteste.

Elemento	Padrão verificável
Responsabilidade	Dono: Segurança da Informação e proprietário do ativo ou serviço. Consultados: Tecnologia, Privacidade, Jurídico, Compliance, Pessoas, Continuidade e gestor do fornecedor. Aprovação/escalonamento: responsável pelo SGSI, Comitê multidisciplinar ou Diretoria para risco residual alto.
Evidência mínima	Registro de entrada, análise, decisão, execução e verificação; conservação em ferramentas oficiais de gestão de ativos, identidade, tickets, logs, monitoramento e riscos com acesso por necessidade.
Indicadores	Percentual de casos conformes; exceções vencidas; tempo de decisão; reincidência; cobertura de treinamento; ações corretivas no prazo.
Teste e alerta	Amostra baseada em risco e revisão após mudança. Escalar imediatamente quando houver comprometimento confirmado ou provável, indisponibilidade crítica, vazamento, perda de evidência, privilégio indevido ou risco residual alto.

Perguntas executivas para aprovação

- A finalidade e a necessidade de governança do sgsi, escopo e apetite a risco estão claras e permanecem válidas?
- Os riscos, pessoas afetadas, dependências, obrigações e possíveis conflitos foram avaliados?
- A evidência produzida permite demonstrar não apenas a existência, mas a efetividade do controle?
- Há condição de parada, prazo de reavaliação e responsável por corrigir eventual resultado adverso?

GATILHO DE PROJETO OU CONTRATO Em novo projeto, produto, fornecedor ou contrato, o tema governança do sgsi, escopo e apetite a risco deve integrar a avaliação de entrada. Se a resposta depender de premissa não confirmada, a aprovação será condicionada; se houver comprometimento confirmado ou provável, indisponibilidade crítica, vazamento, perda de evidência, privilégio indevido ou risco residual alto, o caso seguirá para responsável pelo SGSI, Comitê multidisciplinar ou Diretoria para risco residual alto.

5.C02 Caderno de controle — inventário, propriedade e ciclo de vida de ativos

LEITURA EXECUTIVA Este caderno converte o compromisso sobre inventário, propriedade e ciclo de vida de ativos em uma rotina verificável. Aplica-se a informações, pessoas, equipamentos, aplicações, redes, instalações, serviços em nuvem, fornecedores e ambientes de trabalho remoto e deve ser usado antes da decisão, durante a execução e na revisão de eficácia. O objetivo é permitir que qualquer leitor compreenda o que deve ser feito, quem decide, qual evidência comprova a prática e quando o tema precisa ser escalado.

Objetivo, resultado e critério de aceitação

O resultado esperado para inventário, propriedade e ciclo de vida de ativos é uma decisão coerente com confidencialidade, integridade, disponibilidade, autenticidade, rastreabilidade, ISO/IEC 27001:2022 e controles do Anexo A, baseada em risco, documentada no nível proporcional ao impacto e passível de reconstrução por terceiro independente. O controle é considerado implementado somente quando há responsável designado, critério prévio, execução demonstrável, tratamento de exceções e verificação periódica.

Aplicação operacional mínima

- Planejar: o Segurança da Informação e proprietário do ativo ou serviço define finalidade, entradas, critérios, alçada, prazo e evidência necessária para inventário, propriedade e ciclo de vida de ativos.
- Executar: utilizar fluxo oficial, segregação de funções e validações proporcionais; decisões sensíveis dependem de responsável pelo SGSI, Comitê multidisciplinar ou Diretoria para risco residual alto.
- Registrar: preservar solicitação, análise, aprovação, resultado, comunicação e eventual exceção em ferramentas oficiais de gestão de ativos, identidade, tickets, logs, monitoramento e riscos.
- Verificar: realizar contínua para eventos; mensal, trimestral ou anual conforme criticidade; e após mudança ou incidente teste de desenho e amostra de eficácia, registrando população, seleção, resultado e conclusão.
- Corrigir: desvios devem ser contidos, avaliados quanto à causa, tratados por plano com responsável e submetidos a reteste.

Elemento	Padrão verificável
Responsabilidade	Dono: Segurança da Informação e proprietário do ativo ou serviço. Consultados: Tecnologia, Privacidade, Jurídico, Compliance, Pessoas, Continuidade e gestor do fornecedor. Aprovação/escalonamento: responsável pelo SGSI, Comitê multidisciplinar ou Diretoria para risco residual alto.
Evidência mínima	Registro de entrada, análise, decisão, execução e verificação; conservação em ferramentas oficiais de gestão de ativos, identidade, tickets, logs, monitoramento e riscos com acesso por necessidade.
Indicadores	Percentual de casos conformes; exceções vencidas; tempo de decisão; reincidência; cobertura de treinamento; ações corretivas no prazo.
Teste e alerta	Amostra baseada em risco e revisão após mudança. Escalar imediatamente quando houver comprometimento confirmado ou provável, indisponibilidade crítica, vazamento, perda de evidência, privilégio indevido ou risco residual alto.

Perguntas executivas para aprovação

- A finalidade e a necessidade de inventário, propriedade e ciclo de vida de ativos estão claras e permanecem válidas?
- Os riscos, pessoas afetadas, dependências, obrigações e possíveis conflitos foram avaliados?
- A evidência produzida permite demonstrar não apenas a existência, mas a efetividade do controle?
- Há condição de parada, prazo de reavaliação e responsável por corrigir eventual resultado adverso?

GATILHO DE PROJETO OU CONTRATO Em novo projeto, produto, fornecedor ou contrato, o tema inventário, propriedade e ciclo de vida de ativos deve integrar a avaliação de entrada. Se a resposta depender de premissa não confirmada, a aprovação será condicionada; se houver comprometimento confirmado ou provável, indisponibilidade crítica, vazamento, perda de evidência, privilégio indevido ou risco residual alto, o caso seguirá para responsável pelo SGSI, Comitê multidisciplinar ou Diretoria para risco residual alto.

5.C03 Caderno de controle — classificação, rotulagem e manuseio da informação

LEITURA EXECUTIVA Este caderno converte o compromisso sobre classificação, rotulagem e manuseio da informação em uma rotina verificável. Aplica-se a informações, pessoas, equipamentos, aplicações, redes, instalações, serviços em nuvem, fornecedores e ambientes de trabalho remoto e deve ser usado antes da decisão, durante a execução e na revisão de eficácia. O objetivo é permitir que qualquer leitor compreenda o que deve ser feito, quem decide, qual evidência comprova a prática e quando o tema precisa ser escalado.

Objetivo, resultado e critério de aceitação

O resultado esperado para classificação, rotulagem e manuseio da informação é uma decisão coerente com confidencialidade, integridade, disponibilidade, autenticidade, rastreabilidade, ISO/IEC 27001:2022 e controles do Anexo A, baseada em risco, documentada no nível proporcional ao impacto e passível de reconstrução por terceiro independente. O controle é considerado implementado somente quando há responsável designado, critério prévio, execução demonstrável, tratamento de exceções e verificação periódica.

Aplicação operacional mínima

- Planejar: o Segurança da Informação e proprietário do ativo ou serviço define finalidade, entradas, critérios, alçada, prazo e evidência necessária para classificação, rotulagem e manuseio da informação.
- Executar: utilizar fluxo oficial, segregação de funções e validações proporcionais; decisões sensíveis dependem de responsável pelo SGSI, Comitê multidisciplinar ou Diretoria para risco residual alto.
- Registrar: preservar solicitação, análise, aprovação, resultado, comunicação e eventual exceção em ferramentas oficiais de gestão de ativos, identidade, tickets, logs, monitoramento e riscos.
- Verificar: realizar contínua para eventos; mensal, trimestral ou anual conforme criticidade; e após mudança ou incidente teste de desenho e amostra de eficácia, registrando população, seleção, resultado e conclusão.
- Corrigir: desvios devem ser contidos, avaliados quanto à causa, tratados por plano com responsável e submetidos a reteste.

Elemento	Padrão verificável
Responsabilidade	Dono: Segurança da Informação e proprietário do ativo ou serviço. Consultados: Tecnologia, Privacidade, Jurídico, Compliance, Pessoas, Continuidade e gestor do fornecedor. Aprovação/escalonamento: responsável pelo SGSI, Comitê multidisciplinar ou Diretoria para risco residual alto.
Evidência mínima	Registro de entrada, análise, decisão, execução e verificação; conservação em ferramentas oficiais de gestão de ativos, identidade, tickets, logs, monitoramento e riscos com acesso por necessidade.
Indicadores	Percentual de casos conformes; exceções vencidas; tempo de decisão; reincidência; cobertura de treinamento; ações corretivas no prazo.
Teste e alerta	Amostra baseada em risco e revisão após mudança. Escalar imediatamente quando houver comprometimento confirmado ou provável, indisponibilidade crítica, vazamento, perda de evidência, privilégio indevido ou risco residual alto.

Perguntas executivas para aprovação

- A finalidade e a necessidade de classificação, rotulagem e manuseio da informação estão claras e permanecem válidas?
- Os riscos, pessoas afetadas, dependências, obrigações e possíveis conflitos foram avaliados?
- A evidência produzida permite demonstrar não apenas a existência, mas a efetividade do controle?
- Há condição de parada, prazo de reavaliação e responsável por corrigir eventual resultado adverso?

GATILHO DE PROJETO OU CONTRATO Em novo projeto, produto, fornecedor ou contrato, o tema classificação, rotulagem e manuseio da informação deve integrar a avaliação de entrada. Se a resposta depender de premissa não confirmada, a aprovação será condicionada; se houver comprometimento confirmado ou provável, indisponibilidade crítica, vazamento, perda de evidência, privilégio indevido ou risco residual alto, o caso seguirá para responsável pelo SGSI, Comitê multidisciplinar ou Diretoria para risco residual alto.

5.C04 Caderno de controle — gestão de identidades e acessos

LEITURA EXECUTIVA Este caderno converte o compromisso sobre gestão de identidades e acessos em uma rotina verificável. Aplica-se a informações, pessoas, equipamentos, aplicações, redes, instalações, serviços em nuvem, fornecedores e ambientes de trabalho remoto e deve ser usado antes da decisão, durante a execução e na revisão de eficácia. O objetivo é permitir que qualquer leitor compreenda o que deve ser feito, quem decide, qual evidência comprova a prática e quando o tema precisa ser escalado.

Objetivo, resultado e critério de aceitação

O resultado esperado para gestão de identidades e acessos é uma decisão coerente com confidencialidade, integridade, disponibilidade, autenticidade, rastreabilidade, ISO/IEC 27001:2022 e controles do Anexo A, baseada em risco, documentada no nível proporcional ao impacto e passível de reconstrução por terceiro independente. O controle é considerado implementado somente quando há responsável designado, critério prévio, execução demonstrável, tratamento de exceções e verificação periódica.

Aplicação operacional mínima

- Planejar: o Segurança da Informação e proprietário do ativo ou serviço define finalidade, entradas, critérios, alçada, prazo e evidência necessária para gestão de identidades e acessos.
- Executar: utilizar fluxo oficial, segregação de funções e validações proporcionais; decisões sensíveis dependem de responsável pelo SGSI, Comitê multidisciplinar ou Diretoria para risco residual alto.
- Registrar: preservar solicitação, análise, aprovação, resultado, comunicação e eventual exceção em ferramentas oficiais de gestão de ativos, identidade, tickets, logs, monitoramento e riscos.
- Verificar: realizar contínua para eventos; mensal, trimestral ou anual conforme criticidade; e após mudança ou incidente teste de desenho e amostra de eficácia, registrando população, seleção, resultado e conclusão.
- Corrigir: desvios devem ser contidos, avaliados quanto à causa, tratados por plano com responsável e submetidos a reteste.

Elemento	Padrão verificável
Responsabilidade	Dono: Segurança da Informação e proprietário do ativo ou serviço. Consultados: Tecnologia, Privacidade, Jurídico, Compliance, Pessoas, Continuidade e gestor do fornecedor. Aprovação/escalonamento: responsável pelo SGSI, Comitê multidisciplinar ou Diretoria para risco residual alto.
Evidência mínima	Registro de entrada, análise, decisão, execução e verificação; conservação em ferramentas oficiais de gestão de ativos, identidade, tickets, logs, monitoramento e riscos com acesso por necessidade.
Indicadores	Percentual de casos conformes; exceções vencidas; tempo de decisão; reincidência; cobertura de treinamento; ações corretivas no prazo.
Teste e alerta	Amostra baseada em risco e revisão após mudança. Escalar imediatamente quando houver comprometimento confirmado ou provável, indisponibilidade crítica, vazamento, perda de evidência, privilégio indevido ou risco residual alto.

Perguntas executivas para aprovação

- A finalidade e a necessidade de gestão de identidades e acessos estão claras e permanecem válidas?
- Os riscos, pessoas afetadas, dependências, obrigações e possíveis conflitos foram avaliados?
- A evidência produzida permite demonstrar não apenas a existência, mas a efetividade do controle?
- Há condição de parada, prazo de reavaliação e responsável por corrigir eventual resultado adverso?

GATILHO DE PROJETO OU CONTRATO Em novo projeto, produto, fornecedor ou contrato, o tema gestão de identidades e acessos deve integrar a avaliação de entrada. Se a resposta depender de premissa não confirmada, a aprovação será condicionada; se houver comprometimento confirmado ou provável, indisponibilidade crítica, vazamento, perda de evidência, privilégio indevido ou risco residual alto, o caso seguirá para responsável pelo SGSI, Comitê multidisciplinar ou Diretoria para risco residual alto.

5.C05 Caderno de controle — autenticação multifator e credenciais

LEITURA EXECUTIVA Este caderno converte o compromisso sobre autenticação multifator e credenciais em uma rotina verificável. Aplica-se a informações, pessoas, equipamentos, aplicações, redes, instalações, serviços em nuvem, fornecedores e ambientes de trabalho remoto e deve ser usado antes da decisão, durante a execução e na revisão de eficácia. O objetivo é permitir que qualquer leitor compreenda o que deve ser feito, quem decide, qual evidência comprova a prática e quando o tema precisa ser escalado.

Objetivo, resultado e critério de aceitação

O resultado esperado para autenticação multifator e credenciais é uma decisão coerente com confidencialidade, integridade, disponibilidade, autenticidade, rastreabilidade, ISO/IEC 27001:2022 e controles do Anexo A, baseada em risco, documentada no nível proporcional ao impacto e passível de reconstrução por terceiro independente. O controle é considerado implementado somente quando há responsável designado, critério prévio, execução demonstrável, tratamento de exceções e verificação periódica.

Aplicação operacional mínima

- Planejar: o Segurança da Informação e proprietário do ativo ou serviço define finalidade, entradas, critérios, alçada, prazo e evidência necessária para autenticação multifator e credenciais.
- Executar: utilizar fluxo oficial, segregação de funções e validações proporcionais; decisões sensíveis dependem de responsável pelo SGSI, Comitê multidisciplinar ou Diretoria para risco residual alto.
- Registrar: preservar solicitação, análise, aprovação, resultado, comunicação e eventual exceção em ferramentas oficiais de gestão de ativos, identidade, tickets, logs, monitoramento e riscos.
- Verificar: realizar contínua para eventos; mensal, trimestral ou anual conforme criticidade; e após mudança ou incidente teste de desenho e amostra de eficácia, registrando população, seleção, resultado e conclusão.
- Corrigir: desvios devem ser contidos, avaliados quanto à causa, tratados por plano com responsável e submetidos a reteste.

Elemento	Padrão verificável
Responsabilidade	Dono: Segurança da Informação e proprietário do ativo ou serviço. Consultados: Tecnologia, Privacidade, Jurídico, Compliance, Pessoas, Continuidade e gestor do fornecedor. Aprovação/escalonamento: responsável pelo SGSI, Comitê multidisciplinar ou Diretoria para risco residual alto.
Evidência mínima	Registro de entrada, análise, decisão, execução e verificação; conservação em ferramentas oficiais de gestão de ativos, identidade, tickets, logs, monitoramento e riscos com acesso por necessidade.
Indicadores	Percentual de casos conformes; exceções vencidas; tempo de decisão; reincidência; cobertura de treinamento; ações corretivas no prazo.
Teste e alerta	Amostra baseada em risco e revisão após mudança. Escalar imediatamente quando houver comprometimento confirmado ou provável, indisponibilidade crítica, vazamento, perda de evidência, privilégio indevido ou risco residual alto.

Perguntas executivas para aprovação

- A finalidade e a necessidade de autenticação multifator e credenciais estão claras e permanecem válidas?
- Os riscos, pessoas afetadas, dependências, obrigações e possíveis conflitos foram avaliados?
- A evidência produzida permite demonstrar não apenas a existência, mas a efetividade do controle?
- Há condição de parada, prazo de reavaliação e responsável por corrigir eventual resultado adverso?

GATILHO DE PROJETO OU CONTRATO Em novo projeto, produto, fornecedor ou contrato, o tema autenticação multifator e credenciais deve integrar a avaliação de entrada. Se a resposta depender de premissa não confirmada, a aprovação será condicionada; se houver comprometimento confirmado ou provável, indisponibilidade crítica, vazamento, perda de evidência, privilégio indevido ou risco residual alto, o caso seguirá para responsável pelo SGSI, Comitê multidisciplinar ou Diretoria para risco residual alto.

5.C06 Caderno de controle — acessos privilegiados e contas administrativas

LEITURA EXECUTIVA Este caderno converte o compromisso sobre acessos privilegiados e contas administrativas em uma rotina verificável. Aplica-se a informações, pessoas, equipamentos, aplicações, redes, instalações, serviços em nuvem, fornecedores e ambientes de trabalho remoto e deve ser usado antes da decisão, durante a execução e na revisão de eficácia. O objetivo é permitir que qualquer leitor compreenda o que deve ser feito, quem decide, qual evidência comprova a prática e quando o tema precisa ser escalado.

Objetivo, resultado e critério de aceitação

O resultado esperado para acessos privilegiados e contas administrativas é uma decisão coerente com confidencialidade, integridade, disponibilidade, autenticidade, rastreabilidade, ISO/IEC 27001:2022 e controles do Anexo A, baseada em risco, documentada no nível proporcional ao impacto e passível de reconstrução por terceiro independente. O controle é considerado implementado somente quando há responsável designado, critério prévio, execução demonstrável, tratamento de exceções e verificação periódica.

Aplicação operacional mínima

- Planejar: o Segurança da Informação e proprietário do ativo ou serviço define finalidade, entradas, critérios, alçada, prazo e evidência necessária para acessos privilegiados e contas administrativas.
- Executar: utilizar fluxo oficial, segregação de funções e validações proporcionais; decisões sensíveis dependem de responsável pelo SGSI, Comitê multidisciplinar ou Diretoria para risco residual alto.
- Registrar: preservar solicitação, análise, aprovação, resultado, comunicação e eventual exceção em ferramentas oficiais de gestão de ativos, identidade, tickets, logs, monitoramento e riscos.
- Verificar: realizar contínua para eventos; mensal, trimestral ou anual conforme criticidade; e após mudança ou incidente teste de desenho e amostra de eficácia, registrando população, seleção, resultado e conclusão.
- Corrigir: desvios devem ser contidos, avaliados quanto à causa, tratados por plano com responsável e submetidos a reteste.

Elemento	Padrão verificável
Responsabilidade	Dono: Segurança da Informação e proprietário do ativo ou serviço. Consultados: Tecnologia, Privacidade, Jurídico, Compliance, Pessoas, Continuidade e gestor do fornecedor. Aprovação/escalonamento: responsável pelo SGSI, Comitê multidisciplinar ou Diretoria para risco residual alto.
Evidência mínima	Registro de entrada, análise, decisão, execução e verificação; conservação em ferramentas oficiais de gestão de ativos, identidade, tickets, logs, monitoramento e riscos com acesso por necessidade.
Indicadores	Percentual de casos conformes; exceções vencidas; tempo de decisão; reincidência; cobertura de treinamento; ações corretivas no prazo.
Teste e alerta	Amostra baseada em risco e revisão após mudança. Escalar imediatamente quando houver comprometimento confirmado ou provável, indisponibilidade crítica, vazamento, perda de evidência, privilégio indevido ou risco residual alto.

Perguntas executivas para aprovação

- A finalidade e a necessidade de acessos privilegiados e contas administrativas estão claras e permanecem válidas?
- Os riscos, pessoas afetadas, dependências, obrigações e possíveis conflitos foram avaliados?
- A evidência produzida permite demonstrar não apenas a existência, mas a efetividade do controle?
- Há condição de parada, prazo de reavaliação e responsável por corrigir eventual resultado adverso?

GATILHO DE PROJETO OU CONTRATO Em novo projeto, produto, fornecedor ou contrato, o tema acessos privilegiados e contas administrativas deve integrar a avaliação de entrada. Se a resposta depender de premissa não confirmada, a aprovação será condicionada; se houver comprometimento confirmado ou provável, indisponibilidade crítica, vazamento, perda de evidência, privilégio indevido ou risco residual alto, o caso seguirá para responsável pelo SGSI, Comitê multidisciplinar ou Diretoria para risco residual alto.

5.C07 Caderno de controle — admissão, mudança de função e desligamento

LEITURA EXECUTIVA Este caderno converte o compromisso sobre admissão, mudança de função e desligamento em uma rotina verificável. Aplica-se a informações, pessoas, equipamentos, aplicações, redes, instalações, serviços em nuvem, fornecedores e ambientes de trabalho remoto e deve ser usado antes da decisão, durante a execução e na revisão de eficácia. O objetivo é permitir que qualquer leitor compreenda o que deve ser feito, quem decide, qual evidência comprova a prática e quando o tema precisa ser escalado.

Objetivo, resultado e critério de aceitação

O resultado esperado para admissão, mudança de função e desligamento é uma decisão coerente com confidencialidade, integridade, disponibilidade, autenticidade, rastreabilidade, ISO/IEC 27001:2022 e controles do Anexo A, baseada em risco, documentada no nível proporcional ao impacto e passível de reconstrução por terceiro independente. O controle é considerado implementado somente quando há responsável designado, critério prévio, execução demonstrável, tratamento de exceções e verificação periódica.

Aplicação operacional mínima

- Planejar: o Segurança da Informação e proprietário do ativo ou serviço define finalidade, entradas, critérios, alçada, prazo e evidência necessária para admissão, mudança de função e desligamento.
- Executar: utilizar fluxo oficial, segregação de funções e validações proporcionais; decisões sensíveis dependem de responsável pelo SGSI, Comitê multidisciplinar ou Diretoria para risco residual alto.
- Registrar: preservar solicitação, análise, aprovação, resultado, comunicação e eventual exceção em ferramentas oficiais de gestão de ativos, identidade, tickets, logs, monitoramento e riscos.
- Verificar: realizar contínua para eventos; mensal, trimestral ou anual conforme criticidade; e após mudança ou incidente teste de desenho e amostra de eficácia, registrando população, seleção, resultado e conclusão.
- Corrigir: desvios devem ser contidos, avaliados quanto à causa, tratados por plano com responsável e submetidos a reteste.

Elemento	Padrão verificável
Responsabilidade	Dono: Segurança da Informação e proprietário do ativo ou serviço. Consultados: Tecnologia, Privacidade, Jurídico, Compliance, Pessoas, Continuidade e gestor do fornecedor. Aprovação/escalonamento: responsável pelo SGSI, Comitê multidisciplinar ou Diretoria para risco residual alto.
Evidência mínima	Registro de entrada, análise, decisão, execução e verificação; conservação em ferramentas oficiais de gestão de ativos, identidade, tickets, logs, monitoramento e riscos com acesso por necessidade.
Indicadores	Percentual de casos conformes; exceções vencidas; tempo de decisão; reincidência; cobertura de treinamento; ações corretivas no prazo.
Teste e alerta	Amostra baseada em risco e revisão após mudança. Escalar imediatamente quando houver comprometimento confirmado ou provável, indisponibilidade crítica, vazamento, perda de evidência, privilégio indevido ou risco residual alto.

Perguntas executivas para aprovação

- A finalidade e a necessidade de admissão, mudança de função e desligamento estão claras e permanecem válidas?
- Os riscos, pessoas afetadas, dependências, obrigações e possíveis conflitos foram avaliados?
- A evidência produzida permite demonstrar não apenas a existência, mas a efetividade do controle?
- Há condição de parada, prazo de reavaliação e responsável por corrigir eventual resultado adverso?

GATILHO DE PROJETO OU CONTRATO Em novo projeto, produto, fornecedor ou contrato, o tema admissão, mudança de função e desligamento deve integrar a avaliação de entrada. Se a resposta depender de premissa não confirmada, a aprovação será condicionada; se houver comprometimento confirmado ou provável, indisponibilidade crítica, vazamento, perda de evidência, privilégio indevido ou risco residual alto, o caso seguirá para responsável pelo SGSI, Comitê multidisciplinar ou Diretoria para risco residual alto.

5.C08 Caderno de controle — proteção de endpoints, dispositivos móveis e mídias

LEITURA EXECUTIVA Este caderno converte o compromisso sobre proteção de endpoints, dispositivos móveis e mídias em uma rotina verificável. Aplica-se a informações, pessoas, equipamentos, aplicações, redes, instalações, serviços em nuvem, fornecedores e ambientes de trabalho remoto e deve ser usado antes da decisão, durante a execução e na revisão de eficácia. O objetivo é permitir que qualquer leitor compreenda o que deve ser feito, quem decide, qual evidência comprova a prática e quando o tema precisa ser escalado.

Objetivo, resultado e critério de aceitação

O resultado esperado para proteção de endpoints, dispositivos móveis e mídias é uma decisão coerente com confidencialidade, integridade, disponibilidade, autenticidade, rastreabilidade, ISO/IEC 27001:2022 e controles do Anexo A, baseada em risco, documentada no nível proporcional ao impacto e passível de reconstrução por terceiro independente. O controle é considerado implementado somente quando há responsável designado, critério prévio, execução demonstrável, tratamento de exceções e verificação periódica.

Aplicação operacional mínima

- Planejar: o Segurança da Informação e proprietário do ativo ou serviço define finalidade, entradas, critérios, alçada, prazo e evidência necessária para proteção de endpoints, dispositivos móveis e mídias.
- Executar: utilizar fluxo oficial, segregação de funções e validações proporcionais; decisões sensíveis dependem de responsável pelo SGSI, Comitê multidisciplinar ou Diretoria para risco residual alto.
- Registrar: preservar solicitação, análise, aprovação, resultado, comunicação e eventual exceção em ferramentas oficiais de gestão de ativos, identidade, tickets, logs, monitoramento e riscos.
- Verificar: realizar contínua para eventos; mensal, trimestral ou anual conforme criticidade; e após mudança ou incidente teste de desenho e amostra de eficácia, registrando população, seleção, resultado e conclusão.
- Corrigir: desvios devem ser contidos, avaliados quanto à causa, tratados por plano com responsável e submetidos a reteste.

Elemento	Padrão verificável
Responsabilidade	Dono: Segurança da Informação e proprietário do ativo ou serviço. Consultados: Tecnologia, Privacidade, Jurídico, Compliance, Pessoas, Continuidade e gestor do fornecedor. Aprovação/escalonamento: responsável pelo SGSI, Comitê multidisciplinar ou Diretoria para risco residual alto.
Evidência mínima	Registro de entrada, análise, decisão, execução e verificação; conservação em ferramentas oficiais de gestão de ativos, identidade, tickets, logs, monitoramento e riscos com acesso por necessidade.
Indicadores	Percentual de casos conformes; exceções vencidas; tempo de decisão; reincidência; cobertura de treinamento; ações corretivas no prazo.
Teste e alerta	Amostra baseada em risco e revisão após mudança. Escalar imediatamente quando houver comprometimento confirmado ou provável, indisponibilidade crítica, vazamento, perda de evidência, privilégio indevido ou risco residual alto.

Perguntas executivas para aprovação

- A finalidade e a necessidade de proteção de endpoints, dispositivos móveis e mídias estão claras e permanecem válidas?
- Os riscos, pessoas afetadas, dependências, obrigações e possíveis conflitos foram avaliados?
- A evidência produzida permite demonstrar não apenas a existência, mas a efetividade do controle?
- Há condição de parada, prazo de reavaliação e responsável por corrigir eventual resultado adverso?

GATILHO DE PROJETO OU CONTRATO Em novo projeto, produto, fornecedor ou contrato, o tema proteção de endpoints, dispositivos móveis e mídias deve integrar a avaliação de entrada. Se a resposta depender de premissa não confirmada, a aprovação será condicionada; se houver comprometimento confirmado ou provável, indisponibilidade crítica, vazamento, perda de evidência, privilégio indevido ou risco residual alto, o caso seguirá para responsável pelo SGSI, Comitê multidisciplinar ou Diretoria para risco residual alto.

5.C09 Caderno de controle — configuração segura e hardening

LEITURA EXECUTIVA Este caderno converte o compromisso sobre configuração segura e hardening em uma rotina verificável. Aplica-se a informações, pessoas, equipamentos, aplicações, redes, instalações, serviços em nuvem, fornecedores e ambientes de trabalho remoto e deve ser usado antes da decisão, durante a execução e na revisão de eficácia. O objetivo é permitir que qualquer leitor compreenda o que deve ser feito, quem decide, qual evidência comprova a prática e quando o tema precisa ser escalado.

Objetivo, resultado e critério de aceitação

O resultado esperado para configuração segura e hardening é uma decisão coerente com confidencialidade, integridade, disponibilidade, autenticidade, rastreabilidade, ISO/IEC 27001:2022 e controles do Anexo A, baseada em risco, documentada no nível proporcional ao impacto e passível de reconstrução por terceiro independente. O controle é considerado implementado somente quando há responsável designado, critério prévio, execução demonstrável, tratamento de exceções e verificação periódica.

Aplicação operacional mínima

- Planejar: o Segurança da Informação e proprietário do ativo ou serviço define finalidade, entradas, critérios, alçada, prazo e evidência necessária para configuração segura e hardening.
- Executar: utilizar fluxo oficial, segregação de funções e validações proporcionais; decisões sensíveis dependem de responsável pelo SGSI, Comitê multidisciplinar ou Diretoria para risco residual alto.
- Registrar: preservar solicitação, análise, aprovação, resultado, comunicação e eventual exceção em ferramentas oficiais de gestão de ativos, identidade, tickets, logs, monitoramento e riscos.
- Verificar: realizar contínua para eventos; mensal, trimestral ou anual conforme criticidade; e após mudança ou incidente teste de desenho e amostra de eficácia, registrando população, seleção, resultado e conclusão.
- Corrigir: desvios devem ser contidos, avaliados quanto à causa, tratados por plano com responsável e submetidos a reteste.

Elemento	Padrão verificável
Responsabilidade	Dono: Segurança da Informação e proprietário do ativo ou serviço. Consultados: Tecnologia, Privacidade, Jurídico, Compliance, Pessoas, Continuidade e gestor do fornecedor. Aprovação/escalonamento: responsável pelo SGSI, Comitê multidisciplinar ou Diretoria para risco residual alto.
Evidência mínima	Registro de entrada, análise, decisão, execução e verificação; conservação em ferramentas oficiais de gestão de ativos, identidade, tickets, logs, monitoramento e riscos com acesso por necessidade.
Indicadores	Percentual de casos conformes; exceções vencidas; tempo de decisão; reincidência; cobertura de treinamento; ações corretivas no prazo.
Teste e alerta	Amostra baseada em risco e revisão após mudança. Escalar imediatamente quando houver comprometimento confirmado ou provável, indisponibilidade crítica, vazamento, perda de evidência, privilégio indevido ou risco residual alto.

Perguntas executivas para aprovação

- A finalidade e a necessidade de configuração segura e hardening estão claras e permanecem válidas?
- Os riscos, pessoas afetadas, dependências, obrigações e possíveis conflitos foram avaliados?
- A evidência produzida permite demonstrar não apenas a existência, mas a efetividade do controle?
- Há condição de parada, prazo de reavaliação e responsável por corrigir eventual resultado adverso?

GATILHO DE PROJETO OU CONTRATO Em novo projeto, produto, fornecedor ou contrato, o tema configuração segura e hardening deve integrar a avaliação de entrada. Se a resposta depender de premissa não confirmada, a aprovação será condicionada; se houver comprometimento confirmado ou provável, indisponibilidade crítica, vazamento, perda de evidência, privilégio indevido ou risco residual alto, o caso seguirá para responsável pelo SGSI, Comitê multidisciplinar ou Diretoria para risco residual alto.

5.C10 Caderno de controle — vulnerabilidades, correções e gestão de patches

LEITURA EXECUTIVA Este caderno converte o compromisso sobre vulnerabilidades, correções e gestão de patches em uma rotina verificável. Aplica-se a informações, pessoas, equipamentos, aplicações, redes, instalações, serviços em nuvem, fornecedores e ambientes de trabalho remoto e deve ser usado antes da decisão, durante a execução e na revisão de eficácia. O objetivo é permitir que qualquer leitor compreenda o que deve ser feito, quem decide, qual evidência comprova a prática e quando o tema precisa ser escalado.

Objetivo, resultado e critério de aceitação

O resultado esperado para vulnerabilidades, correções e gestão de patches é uma decisão coerente com confidencialidade, integridade, disponibilidade, autenticidade, rastreabilidade, ISO/IEC 27001:2022 e controles do Anexo A, baseada em risco, documentada no nível proporcional ao impacto e passível de reconstrução por terceiro independente. O controle é considerado implementado somente quando há responsável designado, critério prévio, execução demonstrável, tratamento de exceções e verificação periódica.

Aplicação operacional mínima

- Planejar: o Segurança da Informação e proprietário do ativo ou serviço define finalidade, entradas, critérios, alçada, prazo e evidência necessária para vulnerabilidades, correções e gestão de patches.
- Executar: utilizar fluxo oficial, segregação de funções e validações proporcionais; decisões sensíveis dependem de responsável pelo SGSI, Comitê multidisciplinar ou Diretoria para risco residual alto.
- Registrar: preservar solicitação, análise, aprovação, resultado, comunicação e eventual exceção em ferramentas oficiais de gestão de ativos, identidade, tickets, logs, monitoramento e riscos.
- Verificar: realizar contínua para eventos; mensal, trimestral ou anual conforme criticidade; e após mudança ou incidente teste de desenho e amostra de eficácia, registrando população, seleção, resultado e conclusão.
- Corrigir: desvios devem ser contidos, avaliados quanto à causa, tratados por plano com responsável e submetidos a reteste.

Elemento	Padrão verificável
Responsabilidade	Dono: Segurança da Informação e proprietário do ativo ou serviço. Consultados: Tecnologia, Privacidade, Jurídico, Compliance, Pessoas, Continuidade e gestor do fornecedor. Aprovação/escalonamento: responsável pelo SGSI, Comitê multidisciplinar ou Diretoria para risco residual alto.
Evidência mínima	Registro de entrada, análise, decisão, execução e verificação; conservação em ferramentas oficiais de gestão de ativos, identidade, tickets, logs, monitoramento e riscos com acesso por necessidade.
Indicadores	Percentual de casos conformes; exceções vencidas; tempo de decisão; reincidência; cobertura de treinamento; ações corretivas no prazo.
Teste e alerta	Amostra baseada em risco e revisão após mudança. Escalar imediatamente quando houver comprometimento confirmado ou provável, indisponibilidade crítica, vazamento, perda de evidência, privilégio indevido ou risco residual alto.

Perguntas executivas para aprovação

- A finalidade e a necessidade de vulnerabilidades, correções e gestão de patches estão claras e permanecem válidas?
- Os riscos, pessoas afetadas, dependências, obrigações e possíveis conflitos foram avaliados?
- A evidência produzida permite demonstrar não apenas a existência, mas a efetividade do controle?
- Há condição de parada, prazo de reavaliação e responsável por corrigir eventual resultado adverso?

GATILHO DE PROJETO OU CONTRATO Em novo projeto, produto, fornecedor ou contrato, o tema vulnerabilidades, correções e gestão de patches deve integrar a avaliação de entrada. Se a resposta depender de premissa não confirmada, a aprovação será condicionada; se houver comprometimento confirmado ou provável, indisponibilidade crítica, vazamento, perda de evidência, privilégio indevido ou risco residual alto, o caso seguirá para responsável pelo SGSI, Comitê multidisciplinar ou Diretoria para risco residual alto.

5.C11 Caderno de controle — proteção contra malware, phishing e ransomware

LEITURA EXECUTIVA Este caderno converte o compromisso sobre proteção contra malware, phishing e ransomware em uma rotina verificável. Aplica-se a informações, pessoas, equipamentos, aplicações, redes, instalações, serviços em nuvem, fornecedores e ambientes de trabalho remoto e deve ser usado antes da decisão, durante a execução e na revisão de eficácia. O objetivo é permitir que qualquer leitor compreenda o que deve ser feito, quem decide, qual evidência comprova a prática e quando o tema precisa ser escalado.

Objetivo, resultado e critério de aceitação

O resultado esperado para proteção contra malware, phishing e ransomware é uma decisão coerente com confidencialidade, integridade, disponibilidade, autenticidade, rastreabilidade, ISO/IEC 27001:2022 e controles do Anexo A, baseada em risco, documentada no nível proporcional ao impacto e passível de reconstrução por terceiro independente. O controle é considerado implementado somente quando há responsável designado, critério prévio, execução demonstrável, tratamento de exceções e verificação periódica.

Aplicação operacional mínima

- Planejar: o Segurança da Informação e proprietário do ativo ou serviço define finalidade, entradas, critérios, alçada, prazo e evidência necessária para proteção contra malware, phishing e ransomware.
- Executar: utilizar fluxo oficial, segregação de funções e validações proporcionais; decisões sensíveis dependem de responsável pelo SGSI, Comitê multidisciplinar ou Diretoria para risco residual alto.
- Registrar: preservar solicitação, análise, aprovação, resultado, comunicação e eventual exceção em ferramentas oficiais de gestão de ativos, identidade, tickets, logs, monitoramento e riscos.
- Verificar: realizar contínua para eventos; mensal, trimestral ou anual conforme criticidade; e após mudança ou incidente teste de desenho e amostra de eficácia, registrando população, seleção, resultado e conclusão.
- Corrigir: desvios devem ser contidos, avaliados quanto à causa, tratados por plano com responsável e submetidos a reteste.

Elemento	Padrão verificável
Responsabilidade	Dono: Segurança da Informação e proprietário do ativo ou serviço. Consultados: Tecnologia, Privacidade, Jurídico, Compliance, Pessoas, Continuidade e gestor do fornecedor. Aprovação/escalonamento: responsável pelo SGSI, Comitê multidisciplinar ou Diretoria para risco residual alto.
Evidência mínima	Registro de entrada, análise, decisão, execução e verificação; conservação em ferramentas oficiais de gestão de ativos, identidade, tickets, logs, monitoramento e riscos com acesso por necessidade.
Indicadores	Percentual de casos conformes; exceções vencidas; tempo de decisão; reincidência; cobertura de treinamento; ações corretivas no prazo.
Teste e alerta	Amostra baseada em risco e revisão após mudança. Escalar imediatamente quando houver comprometimento confirmado ou provável, indisponibilidade crítica, vazamento, perda de evidência, privilégio indevido ou risco residual alto.

Perguntas executivas para aprovação

- A finalidade e a necessidade de proteção contra malware, phishing e ransomware estão claras e permanecem válidas?
- Os riscos, pessoas afetadas, dependências, obrigações e possíveis conflitos foram avaliados?
- A evidência produzida permite demonstrar não apenas a existência, mas a efetividade do controle?
- Há condição de parada, prazo de reavaliação e responsável por corrigir eventual resultado adverso?

GATILHO DE PROJETO OU CONTRATO Em novo projeto, produto, fornecedor ou contrato, o tema proteção contra malware, phishing e ransomware deve integrar a avaliação de entrada. Se a resposta depender de premissa não confirmada, a aprovação será condicionada; se houver comprometimento confirmado ou provável, indisponibilidade crítica, vazamento, perda de evidência, privilégio indevido ou risco residual alto, o caso seguirá para responsável pelo SGSI, Comitê multidisciplinar ou Diretoria para risco residual alto.

5.C12 Caderno de controle — segurança de correio, colaboração e navegação

LEITURA EXECUTIVA Este caderno converte o compromisso sobre segurança de correio, colaboração e navegação em uma rotina verificável. Aplica-se a informações, pessoas, equipamentos, aplicações, redes, instalações, serviços em nuvem, fornecedores e ambientes de trabalho remoto e deve ser usado antes da decisão, durante a execução e na revisão de eficácia. O objetivo é permitir que qualquer leitor compreenda o que deve ser feito, quem decide, qual evidência comprova a prática e quando o tema precisa ser escalado.

Objetivo, resultado e critério de aceitação

O resultado esperado para segurança de correio, colaboração e navegação é uma decisão coerente com confidencialidade, integridade, disponibilidade, autenticidade, rastreabilidade, ISO/IEC 27001:2022 e controles do Anexo A, baseada em risco, documentada no nível proporcional ao impacto e passível de reconstrução por terceiro independente. O controle é considerado implementado somente quando há responsável designado, critério prévio, execução demonstrável, tratamento de exceções e verificação periódica.

Aplicação operacional mínima

- Planejar: o Segurança da Informação e proprietário do ativo ou serviço define finalidade, entradas, critérios, alçada, prazo e evidência necessária para segurança de correio, colaboração e navegação.
- Executar: utilizar fluxo oficial, segregação de funções e validações proporcionais; decisões sensíveis dependem de responsável pelo SGSI, Comitê multidisciplinar ou Diretoria para risco residual alto.
- Registrar: preservar solicitação, análise, aprovação, resultado, comunicação e eventual exceção em ferramentas oficiais de gestão de ativos, identidade, tickets, logs, monitoramento e riscos.
- Verificar: realizar contínua para eventos; mensal, trimestral ou anual conforme criticidade; e após mudança ou incidente teste de desenho e amostra de eficácia, registrando população, seleção, resultado e conclusão.
- Corrigir: desvios devem ser contidos, avaliados quanto à causa, tratados por plano com responsável e submetidos a reteste.

Elemento	Padrão verificável
Responsabilidade	Dono: Segurança da Informação e proprietário do ativo ou serviço. Consultados: Tecnologia, Privacidade, Jurídico, Compliance, Pessoas, Continuidade e gestor do fornecedor. Aprovação/escalonamento: responsável pelo SGSI, Comitê multidisciplinar ou Diretoria para risco residual alto.
Evidência mínima	Registro de entrada, análise, decisão, execução e verificação; conservação em ferramentas oficiais de gestão de ativos, identidade, tickets, logs, monitoramento e riscos com acesso por necessidade.
Indicadores	Percentual de casos conformes; exceções vencidas; tempo de decisão; reincidência; cobertura de treinamento; ações corretivas no prazo.
Teste e alerta	Amostra baseada em risco e revisão após mudança. Escalar imediatamente quando houver comprometimento confirmado ou provável, indisponibilidade crítica, vazamento, perda de evidência, privilégio indevido ou risco residual alto.

Perguntas executivas para aprovação

- A finalidade e a necessidade de segurança de correio, colaboração e navegação estão claras e permanecem válidas?
- Os riscos, pessoas afetadas, dependências, obrigações e possíveis conflitos foram avaliados?
- A evidência produzida permite demonstrar não apenas a existência, mas a efetividade do controle?
- Há condição de parada, prazo de reavaliação e responsável por corrigir eventual resultado adverso?

GATILHO DE PROJETO OU CONTRATO Em novo projeto, produto, fornecedor ou contrato, o tema segurança de correio, colaboração e navegação deve integrar a avaliação de entrada. Se a resposta depender de premissa não confirmada, a aprovação será condicionada; se houver comprometimento confirmado ou provável, indisponibilidade crítica, vazamento, perda de evidência, privilégio indevido ou risco residual alto, o caso seguirá para responsável pelo SGSI, Comitê multidisciplinar ou Diretoria para risco residual alto.

5.C13 Caderno de controle — criptografia, certificados e gestão de chaves

LEITURA EXECUTIVA Este caderno converte o compromisso sobre criptografia, certificados e gestão de chaves em uma rotina verificável. Aplica-se a informações, pessoas, equipamentos, aplicações, redes, instalações, serviços em nuvem, fornecedores e ambientes de trabalho remoto e deve ser usado antes da decisão, durante a execução e na revisão de eficácia. O objetivo é permitir que qualquer leitor compreenda o que deve ser feito, quem decide, qual evidência comprova a prática e quando o tema precisa ser escalado.

Objetivo, resultado e critério de aceitação

O resultado esperado para criptografia, certificados e gestão de chaves é uma decisão coerente com confidencialidade, integridade, disponibilidade, autenticidade, rastreabilidade, ISO/IEC 27001:2022 e controles do Anexo A, baseada em risco, documentada no nível proporcional ao impacto e passível de reconstrução por terceiro independente. O controle é considerado implementado somente quando há responsável designado, critério prévio, execução demonstrável, tratamento de exceções e verificação periódica.

Aplicação operacional mínima

- Planejar: o Segurança da Informação e proprietário do ativo ou serviço define finalidade, entradas, critérios, alçada, prazo e evidência necessária para criptografia, certificados e gestão de chaves.
- Executar: utilizar fluxo oficial, segregação de funções e validações proporcionais; decisões sensíveis dependem de responsável pelo SGSI, Comitê multidisciplinar ou Diretoria para risco residual alto.
- Registrar: preservar solicitação, análise, aprovação, resultado, comunicação e eventual exceção em ferramentas oficiais de gestão de ativos, identidade, tickets, logs, monitoramento e riscos.
- Verificar: realizar contínua para eventos; mensal, trimestral ou anual conforme criticidade; e após mudança ou incidente teste de desenho e amostra de eficácia, registrando população, seleção, resultado e conclusão.
- Corrigir: desvios devem ser contidos, avaliados quanto à causa, tratados por plano com responsável e submetidos a reteste.

Elemento	Padrão verificável
Responsabilidade	Dono: Segurança da Informação e proprietário do ativo ou serviço. Consultados: Tecnologia, Privacidade, Jurídico, Compliance, Pessoas, Continuidade e gestor do fornecedor. Aprovação/escalonamento: responsável pelo SGSI, Comitê multidisciplinar ou Diretoria para risco residual alto.
Evidência mínima	Registro de entrada, análise, decisão, execução e verificação; conservação em ferramentas oficiais de gestão de ativos, identidade, tickets, logs, monitoramento e riscos com acesso por necessidade.
Indicadores	Percentual de casos conformes; exceções vencidas; tempo de decisão; reincidência; cobertura de treinamento; ações corretivas no prazo.
Teste e alerta	Amostra baseada em risco e revisão após mudança. Escalar imediatamente quando houver comprometimento confirmado ou provável, indisponibilidade crítica, vazamento, perda de evidência, privilégio indevido ou risco residual alto.

Perguntas executivas para aprovação

- A finalidade e a necessidade de criptografia, certificados e gestão de chaves estão claras e permanecem válidas?
- Os riscos, pessoas afetadas, dependências, obrigações e possíveis conflitos foram avaliados?
- A evidência produzida permite demonstrar não apenas a existência, mas a efetividade do controle?
- Há condição de parada, prazo de reavaliação e responsável por corrigir eventual resultado adverso?

GATILHO DE PROJETO OU CONTRATO Em novo projeto, produto, fornecedor ou contrato, o tema criptografia, certificados e gestão de chaves deve integrar a avaliação de entrada. Se a resposta depender de premissa não confirmada, a aprovação será condicionada; se houver comprometimento confirmado ou provável, indisponibilidade crítica, vazamento, perda de evidência, privilégio indevido ou risco residual alto, o caso seguirá para responsável pelo SGSI, Comitê multidisciplinar ou Diretoria para risco residual alto.

5.C14 Caderno de controle — prevenção contra perda e exfiltração de dados

LEITURA EXECUTIVA Este caderno converte o compromisso sobre prevenção contra perda e exfiltração de dados em uma rotina verificável. Aplica-se a informações, pessoas, equipamentos, aplicações, redes, instalações, serviços em nuvem, fornecedores e ambientes de trabalho remoto e deve ser usado antes da decisão, durante a execução e na revisão de eficácia. O objetivo é permitir que qualquer leitor compreenda o que deve ser feito, quem decide, qual evidência comprova a prática e quando o tema precisa ser escalado.

Objetivo, resultado e critério de aceitação

O resultado esperado para prevenção contra perda e exfiltração de dados é uma decisão coerente com confidencialidade, integridade, disponibilidade, autenticidade, rastreabilidade, ISO/IEC 27001:2022 e controles do Anexo A, baseada em risco, documentada no nível proporcional ao impacto e passível de reconstrução por terceiro independente. O controle é considerado implementado somente quando há responsável designado, critério prévio, execução demonstrável, tratamento de exceções e verificação periódica.

Aplicação operacional mínima

- Planejar: o Segurança da Informação e proprietário do ativo ou serviço define finalidade, entradas, critérios, alçada, prazo e evidência necessária para prevenção contra perda e exfiltração de dados.
- Executar: utilizar fluxo oficial, segregação de funções e validações proporcionais; decisões sensíveis dependem de responsável pelo SGSI, Comitê multidisciplinar ou Diretoria para risco residual alto.
- Registrar: preservar solicitação, análise, aprovação, resultado, comunicação e eventual exceção em ferramentas oficiais de gestão de ativos, identidade, tickets, logs, monitoramento e riscos.
- Verificar: realizar contínua para eventos; mensal, trimestral ou anual conforme criticidade; e após mudança ou incidente teste de desenho e amostra de eficácia, registrando população, seleção, resultado e conclusão.
- Corrigir: desvios devem ser contidos, avaliados quanto à causa, tratados por plano com responsável e submetidos a reteste.

Elemento	Padrão verificável
Responsabilidade	Dono: Segurança da Informação e proprietário do ativo ou serviço. Consultados: Tecnologia, Privacidade, Jurídico, Compliance, Pessoas, Continuidade e gestor do fornecedor. Aprovação/escalonamento: responsável pelo SGSI, Comitê multidisciplinar ou Diretoria para risco residual alto.
Evidência mínima	Registro de entrada, análise, decisão, execução e verificação; conservação em ferramentas oficiais de gestão de ativos, identidade, tickets, logs, monitoramento e riscos com acesso por necessidade.
Indicadores	Percentual de casos conformes; exceções vencidas; tempo de decisão; reincidência; cobertura de treinamento; ações corretivas no prazo.
Teste e alerta	Amostra baseada em risco e revisão após mudança. Escalar imediatamente quando houver comprometimento confirmado ou provável, indisponibilidade crítica, vazamento, perda de evidência, privilégio indevido ou risco residual alto.

Perguntas executivas para aprovação

- A finalidade e a necessidade de prevenção contra perda e exfiltração de dados estão claras e permanecem válidas?
- Os riscos, pessoas afetadas, dependências, obrigações e possíveis conflitos foram avaliados?
- A evidência produzida permite demonstrar não apenas a existência, mas a efetividade do controle?
- Há condição de parada, prazo de reavaliação e responsável por corrigir eventual resultado adverso?

GATILHO DE PROJETO OU CONTRATO Em novo projeto, produto, fornecedor ou contrato, o tema prevenção contra perda e exfiltração de dados deve integrar a avaliação de entrada. Se a resposta depender de premissa não confirmada, a aprovação será condicionada; se houver comprometimento confirmado ou provável, indisponibilidade crítica, vazamento, perda de evidência, privilégio indevido ou risco residual alto, o caso seguirá para responsável pelo SGSI, Comitê multidisciplinar ou Diretoria para risco residual alto.

5.C15 Caderno de controle — backup, restauração e cópias imutáveis

LEITURA EXECUTIVA Este caderno converte o compromisso sobre backup, restauração e cópias imutáveis em uma rotina verificável. Aplica-se a informações, pessoas, equipamentos, aplicações, redes, instalações, serviços em nuvem, fornecedores e ambientes de trabalho remoto e deve ser usado antes da decisão, durante a execução e na revisão de eficácia. O objetivo é permitir que qualquer leitor compreenda o que deve ser feito, quem decide, qual evidência comprova a prática e quando o tema precisa ser escalado.

Objetivo, resultado e critério de aceitação

O resultado esperado para backup, restauração e cópias imutáveis é uma decisão coerente com confidencialidade, integridade, disponibilidade, autenticidade, rastreabilidade, ISO/IEC 27001:2022 e controles do Anexo A, baseada em risco, documentada no nível proporcional ao impacto e passível de reconstrução por terceiro independente. O controle é considerado implementado somente quando há responsável designado, critério prévio, execução demonstrável, tratamento de exceções e verificação periódica.

Aplicação operacional mínima

- Planejar: o Segurança da Informação e proprietário do ativo ou serviço define finalidade, entradas, critérios, alçada, prazo e evidência necessária para backup, restauração e cópias imutáveis.
- Executar: utilizar fluxo oficial, segregação de funções e validações proporcionais; decisões sensíveis dependem de responsável pelo SGSI, Comitê multidisciplinar ou Diretoria para risco residual alto.
- Registrar: preservar solicitação, análise, aprovação, resultado, comunicação e eventual exceção em ferramentas oficiais de gestão de ativos, identidade, tickets, logs, monitoramento e riscos.
- Verificar: realizar contínua para eventos; mensal, trimestral ou anual conforme criticidade; e após mudança ou incidente teste de desenho e amostra de eficácia, registrando população, seleção, resultado e conclusão.
- Corrigir: desvios devem ser contidos, avaliados quanto à causa, tratados por plano com responsável e submetidos a reteste.

Elemento	Padrão verificável
Responsabilidade	Dono: Segurança da Informação e proprietário do ativo ou serviço. Consultados: Tecnologia, Privacidade, Jurídico, Compliance, Pessoas, Continuidade e gestor do fornecedor. Aprovação/escalonamento: responsável pelo SGSI, Comitê multidisciplinar ou Diretoria para risco residual alto.
Evidência mínima	Registro de entrada, análise, decisão, execução e verificação; conservação em ferramentas oficiais de gestão de ativos, identidade, tickets, logs, monitoramento e riscos com acesso por necessidade.
Indicadores	Percentual de casos conformes; exceções vencidas; tempo de decisão; reincidência; cobertura de treinamento; ações corretivas no prazo.
Teste e alerta	Amostra baseada em risco e revisão após mudança. Escalar imediatamente quando houver comprometimento confirmado ou provável, indisponibilidade crítica, vazamento, perda de evidência, privilégio indevido ou risco residual alto.

Perguntas executivas para aprovação

- A finalidade e a necessidade de backup, restauração e cópias imutáveis estão claras e permanecem válidas?
- Os riscos, pessoas afetadas, dependências, obrigações e possíveis conflitos foram avaliados?
- A evidência produzida permite demonstrar não apenas a existência, mas a efetividade do controle?
- Há condição de parada, prazo de reavaliação e responsável por corrigir eventual resultado adverso?

GATILHO DE PROJETO OU CONTRATO Em novo projeto, produto, fornecedor ou contrato, o tema backup, restauração e cópias imutáveis deve integrar a avaliação de entrada. Se a resposta depender de premissa não confirmada, a aprovação será condicionada; se houver comprometimento confirmado ou provável, indisponibilidade crítica, vazamento, perda de evidência, privilégio indevido ou risco residual alto, o caso seguirá para responsável pelo SGSI, Comitê multidisciplinar ou Diretoria para risco residual alto.

5.C16 Caderno de controle — continuidade, recuperação e resiliência operacional

LEITURA EXECUTIVA Este caderno converte o compromisso sobre continuidade, recuperação e resiliência operacional em uma rotina verificável. Aplica-se a informações, pessoas, equipamentos, aplicações, redes, instalações, serviços em nuvem, fornecedores e ambientes de trabalho remoto e deve ser usado antes da decisão, durante a execução e na revisão de eficácia. O objetivo é permitir que qualquer leitor compreenda o que deve ser feito, quem decide, qual evidência comprova a prática e quando o tema precisa ser escalado.

Objetivo, resultado e critério de aceitação

O resultado esperado para continuidade, recuperação e resiliência operacional é uma decisão coerente com confidencialidade, integridade, disponibilidade, autenticidade, rastreabilidade, ISO/IEC 27001:2022 e controles do Anexo A, baseada em risco, documentada no nível proporcional ao impacto e passível de reconstrução por terceiro independente. O controle é considerado implementado somente quando há responsável designado, critério prévio, execução demonstrável, tratamento de exceções e verificação periódica.

Aplicação operacional mínima

- Planejar: o Segurança da Informação e proprietário do ativo ou serviço define finalidade, entradas, critérios, alçada, prazo e evidência necessária para continuidade, recuperação e resiliência operacional.
- Executar: utilizar fluxo oficial, segregação de funções e validações proporcionais; decisões sensíveis dependem de responsável pelo SGSI, Comitê multidisciplinar ou Diretoria para risco residual alto.
- Registrar: preservar solicitação, análise, aprovação, resultado, comunicação e eventual exceção em ferramentas oficiais de gestão de ativos, identidade, tickets, logs, monitoramento e riscos.
- Verificar: realizar contínua para eventos; mensal, trimestral ou anual conforme criticidade; e após mudança ou incidente teste de desenho e amostra de eficácia, registrando população, seleção, resultado e conclusão.
- Corrigir: desvios devem ser contidos, avaliados quanto à causa, tratados por plano com responsável e submetidos a reteste.

Elemento	Padrão verificável
Responsabilidade	Dono: Segurança da Informação e proprietário do ativo ou serviço. Consultados: Tecnologia, Privacidade, Jurídico, Compliance, Pessoas, Continuidade e gestor do fornecedor. Aprovação/escalonamento: responsável pelo SGSI, Comitê multidisciplinar ou Diretoria para risco residual alto.
Evidência mínima	Registro de entrada, análise, decisão, execução e verificação; conservação em ferramentas oficiais de gestão de ativos, identidade, tickets, logs, monitoramento e riscos com acesso por necessidade.
Indicadores	Percentual de casos conformes; exceções vencidas; tempo de decisão; reincidência; cobertura de treinamento; ações corretivas no prazo.
Teste e alerta	Amostra baseada em risco e revisão após mudança. Escalar imediatamente quando houver comprometimento confirmado ou provável, indisponibilidade crítica, vazamento, perda de evidência, privilégio indevido ou risco residual alto.

Perguntas executivas para aprovação

- A finalidade e a necessidade de continuidade, recuperação e resiliência operacional estão claras e permanecem válidas?
- Os riscos, pessoas afetadas, dependências, obrigações e possíveis conflitos foram avaliados?
- A evidência produzida permite demonstrar não apenas a existência, mas a efetividade do controle?
- Há condição de parada, prazo de reavaliação e responsável por corrigir eventual resultado adverso?

GATILHO DE PROJETO OU CONTRATO Em novo projeto, produto, fornecedor ou contrato, o tema continuidade, recuperação e resiliência operacional deve integrar a avaliação de entrada. Se a resposta depender de premissa não confirmada, a aprovação será condicionada; se houver comprometimento confirmado ou provável, indisponibilidade crítica, vazamento, perda de evidência, privilégio indevido ou risco residual alto, o caso seguirá para responsável pelo SGSI, Comitê multidisciplinar ou Diretoria para risco residual alto.

5.C17 Caderno de controle — logs, sincronização, retenção e monitoramento

LEITURA EXECUTIVA Este caderno converte o compromisso sobre logs, sincronização, retenção e monitoramento em uma rotina verificável. Aplica-se a informações, pessoas, equipamentos, aplicações, redes, instalações, serviços em nuvem, fornecedores e ambientes de trabalho remoto e deve ser usado antes da decisão, durante a execução e na revisão de eficácia. O objetivo é permitir que qualquer leitor compreenda o que deve ser feito, quem decide, qual evidência comprova a prática e quando o tema precisa ser escalado.

Objetivo, resultado e critério de aceitação

O resultado esperado para logs, sincronização, retenção e monitoramento é uma decisão coerente com confidencialidade, integridade, disponibilidade, autenticidade, rastreabilidade, ISO/IEC 27001:2022 e controles do Anexo A, baseada em risco, documentada no nível proporcional ao impacto e passível de reconstrução por terceiro independente. O controle é considerado implementado somente quando há responsável designado, critério prévio, execução demonstrável, tratamento de exceções e verificação periódica.

Aplicação operacional mínima

- Planejar: o Segurança da Informação e proprietário do ativo ou serviço define finalidade, entradas, critérios, alçada, prazo e evidência necessária para logs, sincronização, retenção e monitoramento.
- Executar: utilizar fluxo oficial, segregação de funções e validações proporcionais; decisões sensíveis dependem de responsável pelo SGSI, Comitê multidisciplinar ou Diretoria para risco residual alto.
- Registrar: preservar solicitação, análise, aprovação, resultado, comunicação e eventual exceção em ferramentas oficiais de gestão de ativos, identidade, tickets, logs, monitoramento e riscos.
- Verificar: realizar contínua para eventos; mensal, trimestral ou anual conforme criticidade; e após mudança ou incidente teste de desenho e amostra de eficácia, registrando população, seleção, resultado e conclusão.
- Corrigir: desvios devem ser contidos, avaliados quanto à causa, tratados por plano com responsável e submetidos a reteste.

Elemento	Padrão verificável
Responsabilidade	Dono: Segurança da Informação e proprietário do ativo ou serviço. Consultados: Tecnologia, Privacidade, Jurídico, Compliance, Pessoas, Continuidade e gestor do fornecedor. Aprovação/escalonamento: responsável pelo SGSI, Comitê multidisciplinar ou Diretoria para risco residual alto.
Evidência mínima	Registro de entrada, análise, decisão, execução e verificação; conservação em ferramentas oficiais de gestão de ativos, identidade, tickets, logs, monitoramento e riscos com acesso por necessidade.
Indicadores	Percentual de casos conformes; exceções vencidas; tempo de decisão; reincidência; cobertura de treinamento; ações corretivas no prazo.
Teste e alerta	Amostra baseada em risco e revisão após mudança. Escalar imediatamente quando houver comprometimento confirmado ou provável, indisponibilidade crítica, vazamento, perda de evidência, privilégio indevido ou risco residual alto.

Perguntas executivas para aprovação

- A finalidade e a necessidade de logs, sincronização, retenção e monitoramento estão claras e permanecem válidas?
- Os riscos, pessoas afetadas, dependências, obrigações e possíveis conflitos foram avaliados?
- A evidência produzida permite demonstrar não apenas a existência, mas a efetividade do controle?
- Há condição de parada, prazo de reavaliação e responsável por corrigir eventual resultado adverso?

GATILHO DE PROJETO OU CONTRATO Em novo projeto, produto, fornecedor ou contrato, o tema logs, sincronização, retenção e monitoramento deve integrar a avaliação de entrada. Se a resposta depender de premissa não confirmada, a aprovação será condicionada; se houver comprometimento confirmado ou provável, indisponibilidade crítica, vazamento, perda de evidência, privilégio indevido ou risco residual alto, o caso seguirá para responsável pelo SGSI, Comitê multidisciplinar ou Diretoria para risco residual alto.

5.C18 Caderno de controle — detecção, triagem e inteligência de ameaças

LEITURA EXECUTIVA Este caderno converte o compromisso sobre detecção, triagem e inteligência de ameaças em uma rotina verificável. Aplica-se a informações, pessoas, equipamentos, aplicações, redes, instalações, serviços em nuvem, fornecedores e ambientes de trabalho remoto e deve ser usado antes da decisão, durante a execução e na revisão de eficácia. O objetivo é permitir que qualquer leitor compreenda o que deve ser feito, quem decide, qual evidência comprova a prática e quando o tema precisa ser escalado.

Objetivo, resultado e critério de aceitação

O resultado esperado para detecção, triagem e inteligência de ameaças é uma decisão coerente com confidencialidade, integridade, disponibilidade, autenticidade, rastreabilidade, ISO/IEC 27001:2022 e controles do Anexo A, baseada em risco, documentada no nível proporcional ao impacto e passível de reconstrução por terceiro independente. O controle é considerado implementado somente quando há responsável designado, critério prévio, execução demonstrável, tratamento de exceções e verificação periódica.

Aplicação operacional mínima

- Planejar: o Segurança da Informação e proprietário do ativo ou serviço define finalidade, entradas, critérios, alçada, prazo e evidência necessária para detecção, triagem e inteligência de ameaças.
- Executar: utilizar fluxo oficial, segregação de funções e validações proporcionais; decisões sensíveis dependem de responsável pelo SGSI, Comitê multidisciplinar ou Diretoria para risco residual alto.
- Registrar: preservar solicitação, análise, aprovação, resultado, comunicação e eventual exceção em ferramentas oficiais de gestão de ativos, identidade, tickets, logs, monitoramento e riscos.
- Verificar: realizar contínua para eventos; mensal, trimestral ou anual conforme criticidade; e após mudança ou incidente teste de desenho e amostra de eficácia, registrando população, seleção, resultado e conclusão.
- Corrigir: desvios devem ser contidos, avaliados quanto à causa, tratados por plano com responsável e submetidos a reteste.

Elemento	Padrão verificável
Responsabilidade	Dono: Segurança da Informação e proprietário do ativo ou serviço. Consultados: Tecnologia, Privacidade, Jurídico, Compliance, Pessoas, Continuidade e gestor do fornecedor. Aprovação/escalonamento: responsável pelo SGSI, Comitê multidisciplinar ou Diretoria para risco residual alto.
Evidência mínima	Registro de entrada, análise, decisão, execução e verificação; conservação em ferramentas oficiais de gestão de ativos, identidade, tickets, logs, monitoramento e riscos com acesso por necessidade.
Indicadores	Percentual de casos conformes; exceções vencidas; tempo de decisão; reincidência; cobertura de treinamento; ações corretivas no prazo.
Teste e alerta	Amostra baseada em risco e revisão após mudança. Escalar imediatamente quando houver comprometimento confirmado ou provável, indisponibilidade crítica, vazamento, perda de evidência, privilégio indevido ou risco residual alto.

Perguntas executivas para aprovação

- A finalidade e a necessidade de detecção, triagem e inteligência de ameaças estão claras e permanecem válidas?
- Os riscos, pessoas afetadas, dependências, obrigações e possíveis conflitos foram avaliados?
- A evidência produzida permite demonstrar não apenas a existência, mas a efetividade do controle?
- Há condição de parada, prazo de reavaliação e responsável por corrigir eventual resultado adverso?

GATILHO DE PROJETO OU CONTRATO Em novo projeto, produto, fornecedor ou contrato, o tema detecção, triagem e inteligência de ameaças deve integrar a avaliação de entrada. Se a resposta depender de premissa não confirmada, a aprovação será condicionada; se houver comprometimento confirmado ou provável, indisponibilidade crítica, vazamento, perda de evidência, privilégio indevido ou risco residual alto, o caso seguirá para responsável pelo SGSI, Comitê multidisciplinar ou Diretoria para risco residual alto.

5.C19 Caderno de controle — resposta a incidentes e preservação de evidências

LEITURA EXECUTIVA Este caderno converte o compromisso sobre resposta a incidentes e preservação de evidências em uma rotina verificável. Aplica-se a informações, pessoas, equipamentos, aplicações, redes, instalações, serviços em nuvem, fornecedores e ambientes de trabalho remoto e deve ser usado antes da decisão, durante a execução e na revisão de eficácia. O objetivo é permitir que qualquer leitor compreenda o que deve ser feito, quem decide, qual evidência comprova a prática e quando o tema precisa ser escalado.

Objetivo, resultado e critério de aceitação

O resultado esperado para resposta a incidentes e preservação de evidências é uma decisão coerente com confidencialidade, integridade, disponibilidade, autenticidade, rastreabilidade, ISO/IEC 27001:2022 e controles do Anexo A, baseada em risco, documentada no nível proporcional ao impacto e passível de reconstrução por terceiro independente. O controle é considerado implementado somente quando há responsável designado, critério prévio, execução demonstrável, tratamento de exceções e verificação periódica.

Aplicação operacional mínima

- Planejar: o Segurança da Informação e proprietário do ativo ou serviço define finalidade, entradas, critérios, alçada, prazo e evidência necessária para resposta a incidentes e preservação de evidências.
- Executar: utilizar fluxo oficial, segregação de funções e validações proporcionais; decisões sensíveis dependem de responsável pelo SGSI, Comitê multidisciplinar ou Diretoria para risco residual alto.
- Registrar: preservar solicitação, análise, aprovação, resultado, comunicação e eventual exceção em ferramentas oficiais de gestão de ativos, identidade, tickets, logs, monitoramento e riscos.
- Verificar: realizar contínua para eventos; mensal, trimestral ou anual conforme criticidade; e após mudança ou incidente teste de desenho e amostra de eficácia, registrando população, seleção, resultado e conclusão.
- Corrigir: desvios devem ser contidos, avaliados quanto à causa, tratados por plano com responsável e submetidos a reteste.

Elemento	Padrão verificável
Responsabilidade	Dono: Segurança da Informação e proprietário do ativo ou serviço. Consultados: Tecnologia, Privacidade, Jurídico, Compliance, Pessoas, Continuidade e gestor do fornecedor. Aprovação/escalonamento: responsável pelo SGSI, Comitê multidisciplinar ou Diretoria para risco residual alto.
Evidência mínima	Registro de entrada, análise, decisão, execução e verificação; conservação em ferramentas oficiais de gestão de ativos, identidade, tickets, logs, monitoramento e riscos com acesso por necessidade.
Indicadores	Percentual de casos conformes; exceções vencidas; tempo de decisão; reincidência; cobertura de treinamento; ações corretivas no prazo.
Teste e alerta	Amostra baseada em risco e revisão após mudança. Escalar imediatamente quando houver comprometimento confirmado ou provável, indisponibilidade crítica, vazamento, perda de evidência, privilégio indevido ou risco residual alto.

Perguntas executivas para aprovação

- A finalidade e a necessidade de resposta a incidentes e preservação de evidências estão claras e permanecem válidas?
- Os riscos, pessoas afetadas, dependências, obrigações e possíveis conflitos foram avaliados?
- A evidência produzida permite demonstrar não apenas a existência, mas a efetividade do controle?
- Há condição de parada, prazo de reavaliação e responsável por corrigir eventual resultado adverso?

GATILHO DE PROJETO OU CONTRATO Em novo projeto, produto, fornecedor ou contrato, o tema resposta a incidentes e preservação de evidências deve integrar a avaliação de entrada. Se a resposta depender de premissa não confirmada, a aprovação será condicionada; se houver comprometimento confirmado ou provável, indisponibilidade crítica, vazamento, perda de evidência, privilégio indevido ou risco residual alto, o caso seguirá para responsável pelo SGSI, Comitê multidisciplinar ou Diretoria para risco residual alto.

5.C20 Caderno de controle — segurança em nuvem e responsabilidade compartilhada

LEITURA EXECUTIVA Este caderno converte o compromisso sobre segurança em nuvem e responsabilidade compartilhada em uma rotina verificável. Aplica-se a informações, pessoas, equipamentos, aplicações, redes, instalações, serviços em nuvem, fornecedores e ambientes de trabalho remoto e deve ser usado antes da decisão, durante a execução e na revisão de eficácia. O objetivo é permitir que qualquer leitor compreenda o que deve ser feito, quem decide, qual evidência comprova a prática e quando o tema precisa ser escalado.

Objetivo, resultado e critério de aceitação

O resultado esperado para segurança em nuvem e responsabilidade compartilhada é uma decisão coerente com confidencialidade, integridade, disponibilidade, autenticidade, rastreabilidade, ISO/IEC 27001:2022 e controles do Anexo A, baseada em risco, documentada no nível proporcional ao impacto e passível de reconstrução por terceiro independente. O controle é considerado implementado somente quando há responsável designado, critério prévio, execução demonstrável, tratamento de exceções e verificação periódica.

Aplicação operacional mínima

- Planejar: o Segurança da Informação e proprietário do ativo ou serviço define finalidade, entradas, critérios, alçada, prazo e evidência necessária para segurança em nuvem e responsabilidade compartilhada.
- Executar: utilizar fluxo oficial, segregação de funções e validações proporcionais; decisões sensíveis dependem de responsável pelo SGSI, Comitê multidisciplinar ou Diretoria para risco residual alto.
- Registrar: preservar solicitação, análise, aprovação, resultado, comunicação e eventual exceção em ferramentas oficiais de gestão de ativos, identidade, tickets, logs, monitoramento e riscos.
- Verificar: realizar contínua para eventos; mensal, trimestral ou anual conforme criticidade; e após mudança ou incidente teste de desenho e amostra de eficácia, registrando população, seleção, resultado e conclusão.
- Corrigir: desvios devem ser contidos, avaliados quanto à causa, tratados por plano com responsável e submetidos a reteste.

Elemento	Padrão verificável
Responsabilidade	Dono: Segurança da Informação e proprietário do ativo ou serviço. Consultados: Tecnologia, Privacidade, Jurídico, Compliance, Pessoas, Continuidade e gestor do fornecedor. Aprovação/escalonamento: responsável pelo SGSI, Comitê multidisciplinar ou Diretoria para risco residual alto.
Evidência mínima	Registro de entrada, análise, decisão, execução e verificação; conservação em ferramentas oficiais de gestão de ativos, identidade, tickets, logs, monitoramento e riscos com acesso por necessidade.
Indicadores	Percentual de casos conformes; exceções vencidas; tempo de decisão; reincidência; cobertura de treinamento; ações corretivas no prazo.
Teste e alerta	Amostra baseada em risco e revisão após mudança. Escalar imediatamente quando houver comprometimento confirmado ou provável, indisponibilidade crítica, vazamento, perda de evidência, privilégio indevido ou risco residual alto.

Perguntas executivas para aprovação

- A finalidade e a necessidade de segurança em nuvem e responsabilidade compartilhada estão claras e permanecem válidas?
- Os riscos, pessoas afetadas, dependências, obrigações e possíveis conflitos foram avaliados?
- A evidência produzida permite demonstrar não apenas a existência, mas a efetividade do controle?
- Há condição de parada, prazo de reavaliação e responsável por corrigir eventual resultado adverso?

GATILHO DE PROJETO OU CONTRATO Em novo projeto, produto, fornecedor ou contrato, o tema segurança em nuvem e responsabilidade compartilhada deve integrar a avaliação de entrada. Se a resposta depender de premissa não confirmada, a aprovação será condicionada; se houver comprometimento confirmado ou provável, indisponibilidade crítica, vazamento, perda de evidência, privilégio indevido ou risco residual alto, o caso seguirá para responsável pelo SGSI, Comitê multidisciplinar ou Diretoria para risco residual alto.

5.C21 Caderno de controle — seleção, contratação e saída de provedores cloud

LEITURA EXECUTIVA Este caderno converte o compromisso sobre seleção, contratação e saída de provedores cloud em uma rotina verificável. Aplica-se a informações, pessoas, equipamentos, aplicações, redes, instalações, serviços em nuvem, fornecedores e ambientes de trabalho remoto e deve ser usado antes da decisão, durante a execução e na revisão de eficácia. O objetivo é permitir que qualquer leitor compreenda o que deve ser feito, quem decide, qual evidência comprova a prática e quando o tema precisa ser escalado.

Objetivo, resultado e critério de aceitação

O resultado esperado para seleção, contratação e saída de provedores cloud é uma decisão coerente com confidencialidade, integridade, disponibilidade, autenticidade, rastreabilidade, ISO/IEC 27001:2022 e controles do Anexo A, baseada em risco, documentada no nível proporcional ao impacto e passível de reconstrução por terceiro independente. O controle é considerado implementado somente quando há responsável designado, critério prévio, execução demonstrável, tratamento de exceções e verificação periódica.

Aplicação operacional mínima

- Planejar: o Segurança da Informação e proprietário do ativo ou serviço define finalidade, entradas, critérios, alçada, prazo e evidência necessária para seleção, contratação e saída de provedores cloud.
- Executar: utilizar fluxo oficial, segregação de funções e validações proporcionais; decisões sensíveis dependem de responsável pelo SGSI, Comitê multidisciplinar ou Diretoria para risco residual alto.
- Registrar: preservar solicitação, análise, aprovação, resultado, comunicação e eventual exceção em ferramentas oficiais de gestão de ativos, identidade, tickets, logs, monitoramento e riscos.
- Verificar: realizar contínua para eventos; mensal, trimestral ou anual conforme criticidade; e após mudança ou incidente teste de desenho e amostra de eficácia, registrando população, seleção, resultado e conclusão.
- Corrigir: desvios devem ser contidos, avaliados quanto à causa, tratados por plano com responsável e submetidos a reteste.

Elemento	Padrão verificável
Responsabilidade	Dono: Segurança da Informação e proprietário do ativo ou serviço. Consultados: Tecnologia, Privacidade, Jurídico, Compliance, Pessoas, Continuidade e gestor do fornecedor. Aprovação/escalonamento: responsável pelo SGSI, Comitê multidisciplinar ou Diretoria para risco residual alto.
Evidência mínima	Registro de entrada, análise, decisão, execução e verificação; conservação em ferramentas oficiais de gestão de ativos, identidade, tickets, logs, monitoramento e riscos com acesso por necessidade.
Indicadores	Percentual de casos conformes; exceções vencidas; tempo de decisão; reincidência; cobertura de treinamento; ações corretivas no prazo.
Teste e alerta	Amostra baseada em risco e revisão após mudança. Escalar imediatamente quando houver comprometimento confirmado ou provável, indisponibilidade crítica, vazamento, perda de evidência, privilégio indevido ou risco residual alto.

Perguntas executivas para aprovação

- A finalidade e a necessidade de seleção, contratação e saída de provedores cloud estão claras e permanecem válidas?
- Os riscos, pessoas afetadas, dependências, obrigações e possíveis conflitos foram avaliados?
- A evidência produzida permite demonstrar não apenas a existência, mas a efetividade do controle?
- Há condição de parada, prazo de reavaliação e responsável por corrigir eventual resultado adverso?

GATILHO DE PROJETO OU CONTRATO Em novo projeto, produto, fornecedor ou contrato, o tema seleção, contratação e saída de provedores cloud deve integrar a avaliação de entrada. Se a resposta depender de premissa não confirmada, a aprovação será condicionada; se houver comprometimento confirmado ou provável, indisponibilidade crítica, vazamento, perda de evidência, privilégio indevido ou risco residual alto, o caso seguirá para responsável pelo SGSI, Comitê multidisciplinar ou Diretoria para risco residual alto.

5.C22 Caderno de controle — segurança de redes, segmentação e acesso remoto

LEITURA EXECUTIVA Este caderno converte o compromisso sobre segurança de redes, segmentação e acesso remoto em uma rotina verificável. Aplica-se a informações, pessoas, equipamentos, aplicações, redes, instalações, serviços em nuvem, fornecedores e ambientes de trabalho remoto e deve ser usado antes da decisão, durante a execução e na revisão de eficácia. O objetivo é permitir que qualquer leitor compreenda o que deve ser feito, quem decide, qual evidência comprova a prática e quando o tema precisa ser escalado.

Objetivo, resultado e critério de aceitação

O resultado esperado para segurança de redes, segmentação e acesso remoto é uma decisão coerente com confidencialidade, integridade, disponibilidade, autenticidade, rastreabilidade, ISO/IEC 27001:2022 e controles do Anexo A, baseada em risco, documentada no nível proporcional ao impacto e passível de reconstrução por terceiro independente. O controle é considerado implementado somente quando há responsável designado, critério prévio, execução demonstrável, tratamento de exceções e verificação periódica.

Aplicação operacional mínima

- Planejar: o Segurança da Informação e proprietário do ativo ou serviço define finalidade, entradas, critérios, alçada, prazo e evidência necessária para segurança de redes, segmentação e acesso remoto.
- Executar: utilizar fluxo oficial, segregação de funções e validações proporcionais; decisões sensíveis dependem de responsável pelo SGSI, Comitê multidisciplinar ou Diretoria para risco residual alto.
- Registrar: preservar solicitação, análise, aprovação, resultado, comunicação e eventual exceção em ferramentas oficiais de gestão de ativos, identidade, tickets, logs, monitoramento e riscos.
- Verificar: realizar contínua para eventos; mensal, trimestral ou anual conforme criticidade; e após mudança ou incidente teste de desenho e amostra de eficácia, registrando população, seleção, resultado e conclusão.
- Corrigir: desvios devem ser contidos, avaliados quanto à causa, tratados por plano com responsável e submetidos a reteste.

Elemento	Padrão verificável
Responsabilidade	Dono: Segurança da Informação e proprietário do ativo ou serviço. Consultados: Tecnologia, Privacidade, Jurídico, Compliance, Pessoas, Continuidade e gestor do fornecedor. Aprovação/escalonamento: responsável pelo SGSI, Comitê multidisciplinar ou Diretoria para risco residual alto.
Evidência mínima	Registro de entrada, análise, decisão, execução e verificação; conservação em ferramentas oficiais de gestão de ativos, identidade, tickets, logs, monitoramento e riscos com acesso por necessidade.
Indicadores	Percentual de casos conformes; exceções vencidas; tempo de decisão; reincidência; cobertura de treinamento; ações corretivas no prazo.
Teste e alerta	Amostra baseada em risco e revisão após mudança. Escalar imediatamente quando houver comprometimento confirmado ou provável, indisponibilidade crítica, vazamento, perda de evidência, privilégio indevido ou risco residual alto.

Perguntas executivas para aprovação

- A finalidade e a necessidade de segurança de redes, segmentação e acesso remoto estão claras e permanecem válidas?
- Os riscos, pessoas afetadas, dependências, obrigações e possíveis conflitos foram avaliados?
- A evidência produzida permite demonstrar não apenas a existência, mas a efetividade do controle?
- Há condição de parada, prazo de reavaliação e responsável por corrigir eventual resultado adverso?

GATILHO DE PROJETO OU CONTRATO Em novo projeto, produto, fornecedor ou contrato, o tema segurança de redes, segmentação e acesso remoto deve integrar a avaliação de entrada. Se a resposta depender de premissa não confirmada, a aprovação será condicionada; se houver comprometimento confirmado ou provável, indisponibilidade crítica, vazamento, perda de evidência, privilégio indevido ou risco residual alto, o caso seguirá para responsável pelo SGSI, Comitê multidisciplinar ou Diretoria para risco residual alto.

5.C23 Caderno de controle — desenvolvimento seguro, testes e gestão de mudanças

LEITURA EXECUTIVA Este caderno converte o compromisso sobre desenvolvimento seguro, testes e gestão de mudanças em uma rotina verificável. Aplica-se a informações, pessoas, equipamentos, aplicações, redes, instalações, serviços em nuvem, fornecedores e ambientes de trabalho remoto e deve ser usado antes da decisão, durante a execução e na revisão de eficácia. O objetivo é permitir que qualquer leitor compreenda o que deve ser feito, quem decide, qual evidência comprova a prática e quando o tema precisa ser escalado.

Objetivo, resultado e critério de aceitação

O resultado esperado para desenvolvimento seguro, testes e gestão de mudanças é uma decisão coerente com confidencialidade, integridade, disponibilidade, autenticidade, rastreabilidade, ISO/IEC 27001:2022 e controles do Anexo A, baseada em risco, documentada no nível proporcional ao impacto e passível de reconstrução por terceiro independente. O controle é considerado implementado somente quando há responsável designado, critério prévio, execução demonstrável, tratamento de exceções e verificação periódica.

Aplicação operacional mínima

- Planejar: o Segurança da Informação e proprietário do ativo ou serviço define finalidade, entradas, critérios, alçada, prazo e evidência necessária para desenvolvimento seguro, testes e gestão de mudanças.
- Executar: utilizar fluxo oficial, segregação de funções e validações proporcionais; decisões sensíveis dependem de responsável pelo SGSI, Comitê multidisciplinar ou Diretoria para risco residual alto.
- Registrar: preservar solicitação, análise, aprovação, resultado, comunicação e eventual exceção em ferramentas oficiais de gestão de ativos, identidade, tickets, logs, monitoramento e riscos.
- Verificar: realizar contínua para eventos; mensal, trimestral ou anual conforme criticidade; e após mudança ou incidente teste de desenho e amostra de eficácia, registrando população, seleção, resultado e conclusão.
- Corrigir: desvios devem ser contidos, avaliados quanto à causa, tratados por plano com responsável e submetidos a reteste.

Elemento	Padrão verificável
Responsabilidade	Dono: Segurança da Informação e proprietário do ativo ou serviço. Consultados: Tecnologia, Privacidade, Jurídico, Compliance, Pessoas, Continuidade e gestor do fornecedor. Aprovação/escalonamento: responsável pelo SGSI, Comitê multidisciplinar ou Diretoria para risco residual alto.
Evidência mínima	Registro de entrada, análise, decisão, execução e verificação; conservação em ferramentas oficiais de gestão de ativos, identidade, tickets, logs, monitoramento e riscos com acesso por necessidade.
Indicadores	Percentual de casos conformes; exceções vencidas; tempo de decisão; reincidência; cobertura de treinamento; ações corretivas no prazo.
Teste e alerta	Amostra baseada em risco e revisão após mudança. Escalar imediatamente quando houver comprometimento confirmado ou provável, indisponibilidade crítica, vazamento, perda de evidência, privilégio indevido ou risco residual alto.

Perguntas executivas para aprovação

- A finalidade e a necessidade de desenvolvimento seguro, testes e gestão de mudanças estão claras e permanecem válidas?
- Os riscos, pessoas afetadas, dependências, obrigações e possíveis conflitos foram avaliados?
- A evidência produzida permite demonstrar não apenas a existência, mas a efetividade do controle?
- Há condição de parada, prazo de reavaliação e responsável por corrigir eventual resultado adverso?

GATILHO DE PROJETO OU CONTRATO Em novo projeto, produto, fornecedor ou contrato, o tema desenvolvimento seguro, testes e gestão de mudanças deve integrar a avaliação de entrada. Se a resposta depender de premissa não confirmada, a aprovação será condicionada; se houver comprometimento confirmado ou provável, indisponibilidade crítica, vazamento, perda de evidência, privilégio indevido ou risco residual alto, o caso seguirá para responsável pelo SGSI, Comitê multidisciplinar ou Diretoria para risco residual alto.

5.C24 Caderno de controle — fornecedores, cadeia de suprimentos e integrações

LEITURA EXECUTIVA Este caderno converte o compromisso sobre fornecedores, cadeia de suprimentos e integrações em uma rotina verificável. Aplica-se a informações, pessoas, equipamentos, aplicações, redes, instalações, serviços em nuvem, fornecedores e ambientes de trabalho remoto e deve ser usado antes da decisão, durante a execução e na revisão de eficácia. O objetivo é permitir que qualquer leitor compreenda o que deve ser feito, quem decide, qual evidência comprova a prática e quando o tema precisa ser escalado.

Objetivo, resultado e critério de aceitação

O resultado esperado para fornecedores, cadeia de suprimentos e integrações é uma decisão coerente com confidencialidade, integridade, disponibilidade, autenticidade, rastreabilidade, ISO/IEC 27001:2022 e controles do Anexo A, baseada em risco, documentada no nível proporcional ao impacto e passível de reconstrução por terceiro independente. O controle é considerado implementado somente quando há responsável designado, critério prévio, execução demonstrável, tratamento de exceções e verificação periódica.

Aplicação operacional mínima

- Planejar: o Segurança da Informação e proprietário do ativo ou serviço define finalidade, entradas, critérios, alçada, prazo e evidência necessária para fornecedores, cadeia de suprimentos e integrações.
- Executar: utilizar fluxo oficial, segregação de funções e validações proporcionais; decisões sensíveis dependem de responsável pelo SGSI, Comitê multidisciplinar ou Diretoria para risco residual alto.
- Registrar: preservar solicitação, análise, aprovação, resultado, comunicação e eventual exceção em ferramentas oficiais de gestão de ativos, identidade, tickets, logs, monitoramento e riscos.
- Verificar: realizar contínua para eventos; mensal, trimestral ou anual conforme criticidade; e após mudança ou incidente teste de desenho e amostra de eficácia, registrando população, seleção, resultado e conclusão.
- Corrigir: desvios devem ser contidos, avaliados quanto à causa, tratados por plano com responsável e submetidos a reteste.

Elemento	Padrão verificável
Responsabilidade	Dono: Segurança da Informação e proprietário do ativo ou serviço. Consultados: Tecnologia, Privacidade, Jurídico, Compliance, Pessoas, Continuidade e gestor do fornecedor. Aprovação/escalonamento: responsável pelo SGSI, Comitê multidisciplinar ou Diretoria para risco residual alto.
Evidência mínima	Registro de entrada, análise, decisão, execução e verificação; conservação em ferramentas oficiais de gestão de ativos, identidade, tickets, logs, monitoramento e riscos com acesso por necessidade.
Indicadores	Percentual de casos conformes; exceções vencidas; tempo de decisão; reincidência; cobertura de treinamento; ações corretivas no prazo.
Teste e alerta	Amostra baseada em risco e revisão após mudança. Escalar imediatamente quando houver comprometimento confirmado ou provável, indisponibilidade crítica, vazamento, perda de evidência, privilégio indevido ou risco residual alto.

Perguntas executivas para aprovação

- A finalidade e a necessidade de fornecedores, cadeia de suprimentos e integrações estão claras e permanecem válidas?
- Os riscos, pessoas afetadas, dependências, obrigações e possíveis conflitos foram avaliados?
- A evidência produzida permite demonstrar não apenas a existência, mas a efetividade do controle?
- Há condição de parada, prazo de reavaliação e responsável por corrigir eventual resultado adverso?

GATILHO DE PROJETO OU CONTRATO Em novo projeto, produto, fornecedor ou contrato, o tema fornecedores, cadeia de suprimentos e integrações deve integrar a avaliação de entrada. Se a resposta depender de premissa não confirmada, a aprovação será condicionada; se houver comprometimento confirmado ou provável, indisponibilidade crítica, vazamento, perda de evidência, privilégio indevido ou risco residual alto, o caso seguirá para responsável pelo SGSI, Comitê multidisciplinar ou Diretoria para risco residual alto.

5.C25 Caderno de controle — segurança física, visitantes e áreas protegidas

LEITURA EXECUTIVA Este caderno converte o compromisso sobre segurança física, visitantes e áreas protegidas em uma rotina verificável. Aplica-se a informações, pessoas, equipamentos, aplicações, redes, instalações, serviços em nuvem, fornecedores e ambientes de trabalho remoto e deve ser usado antes da decisão, durante a execução e na revisão de eficácia. O objetivo é permitir que qualquer leitor compreenda o que deve ser feito, quem decide, qual evidência comprova a prática e quando o tema precisa ser escalado.

Objetivo, resultado e critério de aceitação

O resultado esperado para segurança física, visitantes e áreas protegidas é uma decisão coerente com confidencialidade, integridade, disponibilidade, autenticidade, rastreabilidade, ISO/IEC 27001:2022 e controles do Anexo A, baseada em risco, documentada no nível proporcional ao impacto e passível de reconstrução por terceiro independente. O controle é considerado implementado somente quando há responsável designado, critério prévio, execução demonstrável, tratamento de exceções e verificação periódica.

Aplicação operacional mínima

- Planejar: o Segurança da Informação e proprietário do ativo ou serviço define finalidade, entradas, critérios, alçada, prazo e evidência necessária para segurança física, visitantes e áreas protegidas.
- Executar: utilizar fluxo oficial, segregação de funções e validações proporcionais; decisões sensíveis dependem de responsável pelo SGSI, Comitê multidisciplinar ou Diretoria para risco residual alto.
- Registrar: preservar solicitação, análise, aprovação, resultado, comunicação e eventual exceção em ferramentas oficiais de gestão de ativos, identidade, tickets, logs, monitoramento e riscos.
- Verificar: realizar contínua para eventos; mensal, trimestral ou anual conforme criticidade; e após mudança ou incidente teste de desenho e amostra de eficácia, registrando população, seleção, resultado e conclusão.
- Corrigir: desvios devem ser contidos, avaliados quanto à causa, tratados por plano com responsável e submetidos a reteste.

Elemento	Padrão verificável
Responsabilidade	Dono: Segurança da Informação e proprietário do ativo ou serviço. Consultados: Tecnologia, Privacidade, Jurídico, Compliance, Pessoas, Continuidade e gestor do fornecedor. Aprovação/escalonamento: responsável pelo SGSI, Comitê multidisciplinar ou Diretoria para risco residual alto.
Evidência mínima	Registro de entrada, análise, decisão, execução e verificação; conservação em ferramentas oficiais de gestão de ativos, identidade, tickets, logs, monitoramento e riscos com acesso por necessidade.
Indicadores	Percentual de casos conformes; exceções vencidas; tempo de decisão; reincidência; cobertura de treinamento; ações corretivas no prazo.
Teste e alerta	Amostra baseada em risco e revisão após mudança. Escalar imediatamente quando houver comprometimento confirmado ou provável, indisponibilidade crítica, vazamento, perda de evidência, privilégio indevido ou risco residual alto.

Perguntas executivas para aprovação

- A finalidade e a necessidade de segurança física, visitantes e áreas protegidas estão claras e permanecem válidas?
- Os riscos, pessoas afetadas, dependências, obrigações e possíveis conflitos foram avaliados?
- A evidência produzida permite demonstrar não apenas a existência, mas a efetividade do controle?
- Há condição de parada, prazo de reavaliação e responsável por corrigir eventual resultado adverso?

GATILHO DE PROJETO OU CONTRATO Em novo projeto, produto, fornecedor ou contrato, o tema segurança física, visitantes e áreas protegidas deve integrar a avaliação de entrada. Se a resposta depender de premissa não confirmada, a aprovação será condicionada; se houver comprometimento confirmado ou provável, indisponibilidade crítica, vazamento, perda de evidência, privilégio indevido ou risco residual alto, o caso seguirá para responsável pelo SGSI, Comitê multidisciplinar ou Diretoria para risco residual alto.

5.C26 Caderno de controle — trabalho remoto e proteção fora das instalações

LEITURA EXECUTIVA Este caderno converte o compromisso sobre trabalho remoto e proteção fora das instalações em uma rotina verificável. Aplica-se a informações, pessoas, equipamentos, aplicações, redes, instalações, serviços em nuvem, fornecedores e ambientes de trabalho remoto e deve ser usado antes da decisão, durante a execução e na revisão de eficácia. O objetivo é permitir que qualquer leitor compreenda o que deve ser feito, quem decide, qual evidência comprova a prática e quando o tema precisa ser escalado.

Objetivo, resultado e critério de aceitação

O resultado esperado para trabalho remoto e proteção fora das instalações é uma decisão coerente com confidencialidade, integridade, disponibilidade, autenticidade, rastreabilidade, ISO/IEC 27001:2022 e controles do Anexo A, baseada em risco, documentada no nível proporcional ao impacto e passível de reconstrução por terceiro independente. O controle é considerado implementado somente quando há responsável designado, critério prévio, execução demonstrável, tratamento de exceções e verificação periódica.

Aplicação operacional mínima

- Planejar: o Segurança da Informação e proprietário do ativo ou serviço define finalidade, entradas, critérios, alçada, prazo e evidência necessária para trabalho remoto e proteção fora das instalações.
- Executar: utilizar fluxo oficial, segregação de funções e validações proporcionais; decisões sensíveis dependem de responsável pelo SGSI, Comitê multidisciplinar ou Diretoria para risco residual alto.
- Registrar: preservar solicitação, análise, aprovação, resultado, comunicação e eventual exceção em ferramentas oficiais de gestão de ativos, identidade, tickets, logs, monitoramento e riscos.
- Verificar: realizar contínua para eventos; mensal, trimestral ou anual conforme criticidade; e após mudança ou incidente teste de desenho e amostra de eficácia, registrando população, seleção, resultado e conclusão.
- Corrigir: desvios devem ser contidos, avaliados quanto à causa, tratados por plano com responsável e submetidos a reteste.

Elemento	Padrão verificável
Responsabilidade	Dono: Segurança da Informação e proprietário do ativo ou serviço. Consultados: Tecnologia, Privacidade, Jurídico, Compliance, Pessoas, Continuidade e gestor do fornecedor. Aprovação/escalonamento: responsável pelo SGSI, Comitê multidisciplinar ou Diretoria para risco residual alto.
Evidência mínima	Registro de entrada, análise, decisão, execução e verificação; conservação em ferramentas oficiais de gestão de ativos, identidade, tickets, logs, monitoramento e riscos com acesso por necessidade.
Indicadores	Percentual de casos conformes; exceções vencidas; tempo de decisão; reincidência; cobertura de treinamento; ações corretivas no prazo.
Teste e alerta	Amostra baseada em risco e revisão após mudança. Escalar imediatamente quando houver comprometimento confirmado ou provável, indisponibilidade crítica, vazamento, perda de evidência, privilégio indevido ou risco residual alto.

Perguntas executivas para aprovação

- A finalidade e a necessidade de trabalho remoto e proteção fora das instalações estão claras e permanecem válidas?
- Os riscos, pessoas afetadas, dependências, obrigações e possíveis conflitos foram avaliados?
- A evidência produzida permite demonstrar não apenas a existência, mas a efetividade do controle?
- Há condição de parada, prazo de reavaliação e responsável por corrigir eventual resultado adverso?

GATILHO DE PROJETO OU CONTRATO Em novo projeto, produto, fornecedor ou contrato, o tema trabalho remoto e proteção fora das instalações deve integrar a avaliação de entrada. Se a resposta depender de premissa não confirmada, a aprovação será condicionada; se houver comprometimento confirmado ou provável, indisponibilidade crítica, vazamento, perda de evidência, privilégio indevido ou risco residual alto, o caso seguirá para responsável pelo SGSI, Comitê multidisciplinar ou Diretoria para risco residual alto.

5.C27 Caderno de controle — uso seguro de inteligência artificial

LEITURA EXECUTIVA Este caderno converte o compromisso sobre uso seguro de inteligência artificial em uma rotina verificável. Aplica-se a informações, pessoas, equipamentos, aplicações, redes, instalações, serviços em nuvem, fornecedores e ambientes de trabalho remoto e deve ser usado antes da decisão, durante a execução e na revisão de eficácia. O objetivo é permitir que qualquer leitor compreenda o que deve ser feito, quem decide, qual evidência comprova a prática e quando o tema precisa ser escalado.

Objetivo, resultado e critério de aceitação

O resultado esperado para uso seguro de inteligência artificial é uma decisão coerente com confidencialidade, integridade, disponibilidade, autenticidade, rastreabilidade, ISO/IEC 27001:2022 e controles do Anexo A, baseada em risco, documentada no nível proporcional ao impacto e passível de reconstrução por terceiro independente. O controle é considerado implementado somente quando há responsável designado, critério prévio, execução demonstrável, tratamento de exceções e verificação periódica.

Aplicação operacional mínima

- Planejar: o Segurança da Informação e proprietário do ativo ou serviço define finalidade, entradas, critérios, alçada, prazo e evidência necessária para uso seguro de inteligência artificial.
- Executar: utilizar fluxo oficial, segregação de funções e validações proporcionais; decisões sensíveis dependem de responsável pelo SGSI, Comitê multidisciplinar ou Diretoria para risco residual alto.
- Registrar: preservar solicitação, análise, aprovação, resultado, comunicação e eventual exceção em ferramentas oficiais de gestão de ativos, identidade, tickets, logs, monitoramento e riscos.
- Verificar: realizar contínua para eventos; mensal, trimestral ou anual conforme criticidade; e após mudança ou incidente teste de desenho e amostra de eficácia, registrando população, seleção, resultado e conclusão.
- Corrigir: desvios devem ser contidos, avaliados quanto à causa, tratados por plano com responsável e submetidos a reteste.

Elemento	Padrão verificável
Responsabilidade	Dono: Segurança da Informação e proprietário do ativo ou serviço. Consultados: Tecnologia, Privacidade, Jurídico, Compliance, Pessoas, Continuidade e gestor do fornecedor. Aprovação/escalonamento: responsável pelo SGSI, Comitê multidisciplinar ou Diretoria para risco residual alto.
Evidência mínima	Registro de entrada, análise, decisão, execução e verificação; conservação em ferramentas oficiais de gestão de ativos, identidade, tickets, logs, monitoramento e riscos com acesso por necessidade.
Indicadores	Percentual de casos conformes; exceções vencidas; tempo de decisão; reincidência; cobertura de treinamento; ações corretivas no prazo.
Teste e alerta	Amostra baseada em risco e revisão após mudança. Escalar imediatamente quando houver comprometimento confirmado ou provável, indisponibilidade crítica, vazamento, perda de evidência, privilégio indevido ou risco residual alto.

Perguntas executivas para aprovação

- A finalidade e a necessidade de uso seguro de inteligência artificial estão claras e permanecem válidas?
- Os riscos, pessoas afetadas, dependências, obrigações e possíveis conflitos foram avaliados?
- A evidência produzida permite demonstrar não apenas a existência, mas a efetividade do controle?
- Há condição de parada, prazo de reavaliação e responsável por corrigir eventual resultado adverso?

GATILHO DE PROJETO OU CONTRATO Em novo projeto, produto, fornecedor ou contrato, o tema uso seguro de inteligência artificial deve integrar a avaliação de entrada. Se a resposta depender de premissa não confirmada, a aprovação será condicionada; se houver comprometimento confirmado ou provável, indisponibilidade crítica, vazamento, perda de evidência, privilégio indevido ou risco residual alto, o caso seguirá para responsável pelo SGSI, Comitê multidisciplinar ou Diretoria para risco residual alto.

5.C28 Caderno de controle — métricas, auditoria, testes e melhoria do SGSI

LEITURA EXECUTIVA Este caderno converte o compromisso sobre métricas, auditoria, testes e melhoria do sgsi em uma rotina verificável. Aplica-se a informações, pessoas, equipamentos, aplicações, redes, instalações, serviços em nuvem, fornecedores e ambientes de trabalho remoto e deve ser usado antes da decisão, durante a execução e na revisão de eficácia. O objetivo é permitir que qualquer leitor compreenda o que deve ser feito, quem decide, qual evidência comprova a prática e quando o tema precisa ser escalado.

Objetivo, resultado e critério de aceitação

O resultado esperado para métricas, auditoria, testes e melhoria do sgsi é uma decisão coerente com confidencialidade, integridade, disponibilidade, autenticidade, rastreabilidade, ISO/IEC 27001:2022 e controles do Anexo A, baseada em risco, documentada no nível proporcional ao impacto e passível de reconstrução por terceiro independente. O controle é considerado implementado somente quando há responsável designado, critério prévio, execução demonstrável, tratamento de exceções e verificação periódica.

Aplicação operacional mínima

- Planejar: o Segurança da Informação e proprietário do ativo ou serviço define finalidade, entradas, critérios, alçada, prazo e evidência necessária para métricas, auditoria, testes e melhoria do sgsi.
- Executar: utilizar fluxo oficial, segregação de funções e validações proporcionais; decisões sensíveis dependem de responsável pelo SGSI, Comitê multidisciplinar ou Diretoria para risco residual alto.
- Registrar: preservar solicitação, análise, aprovação, resultado, comunicação e eventual exceção em ferramentas oficiais de gestão de ativos, identidade, tickets, logs, monitoramento e riscos.
- Verificar: realizar contínua para eventos; mensal, trimestral ou anual conforme criticidade; e após mudança ou incidente teste de desenho e amostra de eficácia, registrando população, seleção, resultado e conclusão.
- Corrigir: desvios devem ser contidos, avaliados quanto à causa, tratados por plano com responsável e submetidos a reteste.

Elemento	Padrão verificável
Responsabilidade	Dono: Segurança da Informação e proprietário do ativo ou serviço. Consultados: Tecnologia, Privacidade, Jurídico, Compliance, Pessoas, Continuidade e gestor do fornecedor. Aprovação/escalonamento: responsável pelo SGSI, Comitê multidisciplinar ou Diretoria para risco residual alto.
Evidência mínima	Registro de entrada, análise, decisão, execução e verificação; conservação em ferramentas oficiais de gestão de ativos, identidade, tickets, logs, monitoramento e riscos com acesso por necessidade.
Indicadores	Percentual de casos conformes; exceções vencidas; tempo de decisão; reincidência; cobertura de treinamento; ações corretivas no prazo.
Teste e alerta	Amostra baseada em risco e revisão após mudança. Escalar imediatamente quando houver comprometimento confirmado ou provável, indisponibilidade crítica, vazamento, perda de evidência, privilégio indevido ou risco residual alto.

Perguntas executivas para aprovação

- A finalidade e a necessidade de métricas, auditoria, testes e melhoria do sgsi estão claras e permanecem válidas?
- Os riscos, pessoas afetadas, dependências, obrigações e possíveis conflitos foram avaliados?
- A evidência produzida permite demonstrar não apenas a existência, mas a efetividade do controle?
- Há condição de parada, prazo de reavaliação e responsável por corrigir eventual resultado adverso?

GATILHO DE PROJETO OU CONTRATO Em novo projeto, produto, fornecedor ou contrato, o tema métricas, auditoria, testes e melhoria do sgsi deve integrar a avaliação de entrada. Se a resposta depender de premissa não confirmada, a aprovação será condicionada; se houver comprometimento confirmado ou provável, indisponibilidade crítica, vazamento, perda de evidência, privilégio indevido ou risco residual alto, o caso seguirá para responsável pelo SGSI, Comitê multidisciplinar ou Diretoria para risco residual alto.

6. Potenciais Registros que podem Ser Gerados

Os registros abaixo são potenciais evidências de execução. A retenção indicada é recomendação mínima e deve ser ajustada pelo inventário de dados, tabela de temporalidade, obrigação legal, ordem de preservação, contrato e necessidade de defesa de direitos. Registros sujeitos a sigilo profissional ou legal exigem segregação e acesso por necessidade de conhecer.

Registro / Evidência	Tipo	Responsável (Área dona)	Local oficial	Proteção (mínimo)	Contém dados pessoais?	Retenção mínima (recom.)	Disposição final	Classificação	Descarte seguro	Observações de conformidade
Inventário de ativos e software	Inventário	TI + proprietários	CMDB/repositório SGSI	MFA, logs e backup	Possivelmente	Vida do ativo + 5 anos	Eliminar após baixa	Confidencial	Exclusão/sanitização	Revisão semestral; incluir nuvem, remoto, versão, proprietário e status.
Matriz de riscos e SoA	Matriz	Segurança + Comitê	Repositório SGSI	Versão, aprovação e acesso	Possivelmente	Vigência + 5 anos	Eliminar após prazo/hold	Restrito	Exclusão segura	Justificar inclusão/exclusão de controles e risco residual.
Solicitações e revisões de acesso	Log/processo	TI + proprietário	IAM/chamados	Integridade, MFA e trilha	Sim	Vínculo/conta + 5 anos	Eliminar após prazo	Confidencial	Exclusão segura	Cobrir concessão, alteração, revisão e revogação.
Logs de segurança e auditoria	Log técnico	Segurança/TI	SIEM/log store	Imutabilidade, criptografia e acesso	Possivelmente	Conforme risco; mínimo definido por fonte	Expurgo automatizado	Restrito	Exclusão criptográfica	Minimizar conteúdo; sincronizar tempo e testar alertas.
Scans, patches e pentests	Relatório/ticket	Segurança + TI	Plataforma de vulnerabilidades	Segregação, integridade e hold	Possivelmente	5 anos	Eliminar após prazo/hold	Altamente restrito	Exclusão segura	Registrar severidade, SLA, evidência de correção e reteste.
Backups e testes de restauração	Log/relatório	TI + proprietário	Plataforma de backup	Criptografia, imutabilidade e acesso	Sim	Conforme política e RPO	Expurgo seguro	Altamente restrito	Exclusão criptográfica	Não usar backup como arquivo eterno; testar restauração.
Incidentes e cadeia de custódia	Dossiê	Segurança + DPO/Jurídico	Repositório de incidentes	Need-to-know, hash, logs e hold	Sim	Mínimo 5 anos; ajustar	Eliminar após prazo/hold	Altamente restrito	Exclusão certificada	Preservar cronologia, decisões, evidências, comunicações e lições.
Avaliação e contratos de cloud/fornecedores	Dossiê	TI + Compras + DPO	ECM contratual	Perfis, versão e assinatura	Possivelmente	Contrato + 10 anos	Eliminar após prazo/hold	Restrito	Trituração/exclusão segura	Regiões, suboperadores, SLA, saída, incidentes e responsabilidades.
Treinamento e simulações	Certificado/log	Segurança + Pessoas	Academy Volk	Conta individual e trilha	Sim	Vínculo + 5 anos	Eliminar/anonimizar	Interno	Exclusão segura	Ingresso, anual e por risco; métricas sem exposição indevida.

FECHAMENTO O proprietário do documento deve verificar, na revisão anual, se os registros estão sendo produzidos, protegidos, retidos e descartados conforme definido. Lacunas devem gerar plano de ação com responsável e prazo.