MA-002 - Manual de Segurança da Informação (PSI)

MA-002 - Manual de Segurança da Informação (PSI)

Controle de Versões do Documento

Versão	Data	Elaborador	Revisor/Aprovador	Descrição da alteração
1.0	01/03/2026	Comitê Multidisciplinar	Diretoria	Versão anterior do MA-002, substituída por esta revisão integral.
2.0	10/07/2026	Comitê Multidisciplinar do SGI	Diretoria	Reelaboração integral do Manual e da Política de Segurança da Informação, alinhada à ISO/IEC 27001:2022 com Emenda 1:2024, ao contexto de registradora de contratos de veículos, à estrutura tecnológica

				simplificada, aos datacenters/nuvem contratados e aos achados de auditoria interna, análise crítica e planos de ação do SGI.

Informações sobre a Utilização e o Controle do Documento

Importante: este documento, quando impresso, exportado, copiado para unidade local, encaminhado por e-mail ou reproduzido fora do repositório eletrônico oficial, é considerado **cópia não controlada**, salvo quando houver identificação expressa de cópia controlada, responsável, finalidade, prazo de validade e controle de distribuição.

A versão válida deve ser consultada exclusivamente no canal oficial da 1 IT, disponível no **Outline Wiki corporativo**, ou em outro Enterprise Content Manager formalmente aprovado pela Alta Direção. Os usuários devem verificar código, versão, data, aprovação, classificação e vigência antes de utilizar o conteúdo.

Nenhuma credencial, senha, token, chave de API, segredo criptográfico, certificado privado, código de recuperação ou informação equivalente pode ser inserida neste Manual, em páginas amplamente acessíveis do Outline, em tickets sem proteção adequada ou em comunicações não autorizadas. Chaves utilizadas em integrações ou consultas devem ser limitadas por escopo, possuir validade definida, ser armazenadas em cofre de segredos e ser rotacionadas após exposição, suspeita de comprometimento, mudança de responsável ou encerramento da finalidade.

Este Manual contém uma **interpretação operacional e paráfrases** de requisitos e controles normativos. Ele não reproduz nem substitui as normas oficiais, que devem ser adquiridas e consultadas em suas versões vigentes.

Declaração Institucional da Política de Segurança da Informação

A 1 IT reconhece a informação, os dados pessoais, os registros de contratos, as integrações, os sistemas, as credenciais, os códigos, os logs, os documentos, os serviços em nuvem e a reputação institucional como ativos essenciais para a continuidade do negócio, para a confiança de clientes e parceiros e para o atendimento de obrigações legais, regulatórias e contratuais.

A Alta Direção estabelece que todas as pessoas que atuem em nome da 1 IT devem proteger a **confidencialidade, integridade, disponibilidade, autenticidade, rastreabilidade e privacidade** das informações, observando o princípio do menor

privilégio, a necessidade de conhecimento, a segregação de funções, a defesa em profundidade, a segurança e privacidade desde a concepção, a gestão baseada em riscos e a melhoria contínua.

São compromissos institucionais da 1 IT:

1. manter e melhorar continuamente o Sistema de Gestão da Segurança da Informação - SGSI;
2. atender requisitos legais, regulatórios, contratuais, de credenciamento e de partes interessadas aplicáveis;
3. identificar, avaliar, tratar, aceitar e monitorar riscos de segurança da informação de forma documentada;
4. selecionar controles coerentes com os riscos e manter uma Declaração de Aplicabilidade atualizada;
5. proteger dados e serviços em todo o ciclo de vida, inclusive em fornecedores, suboperadores, datacenters, nuvem e integrações;
6. manter mecanismos de prevenção, detecção, resposta, recuperação e aprendizado com incidentes;
7. capacitar colaboradores e terceiros, mantendo treinamento inicial, integração anual em EAD, avaliações e termos de ciência;
8. assegurar recursos, competências, responsabilidades e autoridade para o funcionamento do SGSI;
9. medir o desempenho dos controles, executar auditorias internas e realizar análise crítica pela Direção;
10. tratar desvios, não conformidades e oportunidades de melhoria com causa, plano de ação e verificação de eficácia.

O descumprimento desta Política pode resultar em revogação de acessos, medidas administrativas e disciplinares, responsabilização contratual e comunicação às autoridades competentes, conforme a natureza e gravidade do evento, assegurados os direitos aplicáveis e a apuração imparcial.

---

1. Apresentação, Finalidade e Escopo

1.1 Finalidade

Este Manual estabelece a Política de Segurança da Informação da 1 IT e organiza as diretrizes, responsabilidades, processos, controles, evidências e critérios mínimos para estabelecer, implementar, manter e melhorar continuamente o SGSI.

O documento foi elaborado para substituir a versão anterior do MA-002 e para apoiar a operação, a auditoria interna, a análise crítica, a preparação para certificação, o

relacionamento com clientes e órgãos reguladores e a demonstração objetiva de conformidade.

1.2 Objetivos específicos

- proteger informações e ativos contra acesso, uso, alteração, divulgação, interrupção, destruição ou perda não autorizada;
- assegurar segurança e rastreabilidade nos processos de registro de contratos de veículos, integrações, atendimento, suporte e atividades administrativas correlatas;
- integrar segurança da informação, privacidade, continuidade, compliance, gestão de fornecedores, desenvolvimento e governança de tecnologia;
- definir critérios consistentes para riscos, acessos, classificação, criptografia, logs, backup, vulnerabilidades, mudanças e incidentes;
- atribuir papéis, responsabilidades, autoridades e alçadas de aprovação;
- estabelecer registros e evidências auditáveis, evitando que controles existam apenas de forma declaratória;
- orientar a seleção e a implementação dos controles do Anexo A da ISO/IEC 27001:2022;
- apoiar o fechamento das ações RNC-001 a RNC-006 e a comprovação de eficácia antes e após a auditoria externa.

1.3 Contexto institucional e modelo de negócio

A 1 IT é uma empresa de tecnologia que atua em soluções digitais, integrações, automação de processos, serviços em nuvem e atividades relacionadas à operação como registradora de contratos de veículos. O escopo definitivo de produtos, credenciamentos, estados atendidos, sistemas e integrações deve permanecer alinhado ao cadastro societário, aos contratos, às autorizações regulatórias, ao website institucional e ao escopo aprovado do SGI.

A operação depende principalmente de sistemas, APIs, bancos de dados, credenciais, certificados, conectividade, logs, backups, serviços em nuvem/datacenters contratados, fornecedores especializados e equipe habilitada. A sede física possui finalidade predominantemente administrativa e de recepção, sem premissa de processamento crítico ou datacenter próprio.

A comunicação pública da 1 IT apresenta compromissos com plataforma segura, uso de cloud computing, criptografia e acesso limitado a pessoas habilitadas. Tais declarações devem ser sustentadas por configurações, contratos, testes, relatórios, registros e controles efetivamente implantados.

1.4 Escopo do SGSI

O SGSI aplica-se aos processos, pessoas, informações, tecnologias, instalações, fornecedores e interfaces necessários à prestação e sustentação dos serviços da 1 IT,

incluindo, conforme aplicável:

- recepção, validação, processamento, registro, transmissão, consulta e guarda de informações vinculadas a contratos de veículos;
- relacionamento e integrações com clientes, credoras, órgãos de trânsito, parceiros, registradoras, fornecedores e demais partes autorizadas;
- aplicações web, portais, APIs, microsserviços, bancos de dados, filas, armazenamento, logs, repositórios de código e ferramentas de suporte;
- ambientes de desenvolvimento, teste, homologação, produção, contingência, nuvem e datacenter;
- gestão de acessos, identidades, privilégios, certificados, chaves, segredos e contas técnicas;
- atendimento, suporte, gestão de incidentes, continuidade, mudanças, vulnerabilidades, backup e recuperação;
- documentos e registros do SGI mantidos no Outline Wiki e em repositórios complementares controlados;
- tratamento de dados pessoais realizado como controladora, operadora/processadora, suboperadora ou controladora conjunta, conforme o fluxo e a relação contratual;
- fornecedores críticos, serviços terceirizados e cadeias de suprimentos de tecnologia que possam afetar o SGSI.

1.4.1 Limites e exclusões justificáveis

Ativos pessoais de colaboradores não integram o escopo, exceto quando formalmente autorizados para trabalho remoto ou BYOD. Sistemas de terceiros fora do controle direto da 1 IT permanecem sujeitos à gestão de requisitos, riscos, contratos, monitoramento, incidentes e continuidade nas interfaces sob responsabilidade da organização.

Nenhuma exclusão pode ser utilizada para afastar responsabilidade sobre processo terceirizado, tratamento de dados, obrigação contratual, integração, credencial, configuração, evidência ou decisão sob governança da 1 IT.

1.5 Abrangência e público-alvo

Este Manual é obrigatório para a Alta Direção, colaboradores, estagiários, prestadores, consultores, auditores, parceiros, fornecedores e quaisquer pessoas que tenham acesso a informações, sistemas, ambientes, ativos ou processos da 1 IT. Requisitos específicos devem ser incorporados aos contratos e termos aplicáveis.

1.6 Critérios de interpretação

- **Deve** indica requisito obrigatório da 1 IT.

- **Deveria** indica prática recomendada, cuja não adoção exige avaliação e justificativa de risco.
- **Pode** indica alternativa permitida, sujeita a alçada e controles aplicáveis.
- **Aplicável por responsabilidade compartilhada** indica controle executado parcialmente pela 1 IT e parcialmente por provedor, sem transferência integral da responsabilidade de governança.
- Em caso de conflito, prevalecem a lei, a regulação, o contrato mais restritivo, a decisão formal da Alta Direção e a versão vigente do documento específico, nessa ordem, após análise jurídica e do SGI.

2. Referências Normativas, Legais e Documentais

2.1 Referências normativas e técnicas

- ISO/IEC 27001:2022 - requisitos para Sistemas de Gestão da Segurança da Informação;
- ISO/IEC 27001:2022/Amd 1:2024 - consideração de mudanças climáticas no contexto e nas partes interessadas;
- ISO/IEC 27002:2022 - orientações para controles de segurança da informação;
- ISO/IEC 27005:2022 - gestão de riscos de segurança da informação;
- ISO/IEC 27017 - controles de segurança para serviços em nuvem;
- ISO/IEC 27018 - proteção de dados pessoais em nuvens públicas;
- ISO/IEC 27701:2025 - Sistema de Gestão de Informações de Privacidade, observada a versão ABNT adotada e o critério do organismo certificador;
- ISO 22301:2019 e Emenda 1:2024 - Sistema de Gestão de Continuidade de Negócios;
- ISO 31000:2018 - princípios e diretrizes de gestão de riscos;
- ISO 19011:2018 - diretrizes para auditoria de sistemas de gestão;
- OWASP ASVS, OWASP API Security Top 10 e OWASP Top 10, quando aplicáveis ao desenvolvimento e às integrações;
- NIST Cybersecurity Framework e CIS Controls, como referências complementares, sem substituição dos requisitos normativos adotados.

2.2 Referências legais, regulatórias e contratuais

- Lei nº 13.709/2018 - Lei Geral de Proteção de Dados Pessoais - LGPD;
- Lei nº 12.965/2014 - Marco Civil da Internet, e regulamentação aplicável;
- Lei nº 14.063/2020, quando aplicável a assinaturas eletrônicas;
- regulamentações, guias e decisões da Autoridade Nacional de Proteção de Dados - ANPD;

- normas, portarias, manuais, requisitos de credenciamento e determinações de órgãos de trânsito e entidades reguladoras aplicáveis à atividade de registro de contratos;
- contratos, editais, SLAs, DPAs, termos de confidencialidade, acordos de tratamento, instruções documentadas de controladores e requisitos de clientes;
- obrigações societárias, fiscais, trabalhistas, consumeristas, de propriedade intelectual, segurança cibernética e preservação de evidências aplicáveis.

2.3 Documentos internos relacionados

Código/Referência	Documento	Relação com este Manual
MA-001	Manual de Funções da 1 IT	Papéis, responsabilidades, substituições, competências e segregação de funções.
MA-002	Manual de Segurança da Informação (PSI)	Documento central do SGSI e desta revisão.
MA-003	Manual de Anticorrupção e Compliance	Integração de integridade, fornecedores, denúncias, investigações e controles de terceiros.
MA-004	Manual de Proteção de Dados (LGPD)	Integração do SGSI com o SGPI, dados pessoais, titulares, incidentes e accountability.
MA-004-MD	Mapa de Dados Completo	Inventário de operações de tratamento, sistemas, compartilhamentos, retenção e agentes de tratamento.
MA-004-AIPD	AIPD/RIPD - Controlador e Operador/Processador	Riscos de privacidade, medidas de segurança e decisões sobre risco residual.
Contratos/DPAs/NDAs	Instrumentos com fornecedores, clientes e parceiros	Cláusulas de segurança, privacidade, continuidade, incidentes, auditoria, subcontratação e reversibilidade.
Análise de Datacenters Tier III	Avaliação de infraestrutura contratada	Criticidade, certificações, redundância, continuidade,

		segurança física e evidências de fornecedores.

2.4 Hierarquia documental do SGSI

Nível	Tipo	Finalidade	Exemplos
1	Política e Manual	Define princípios, compromissos, governança e requisitos institucionais.	MA-002, políticas corporativas.
2	Procedimento Operacional	Define fluxo, papéis, critérios, entradas, saídas e registros de processos.	PO-004, PO-014, PO-016.
3	Instrução de Trabalho	Detalha execução técnica ou operacional.	Hardening, restauração, criação de usuário, coleta de logs.
4	Formulário, checklist e modelo	Padroniza coleta, aprovação e evidência.	Registro de risco, acesso, mudança, incidente, fornecedor.
5	Registro e evidência	Demonstra execução e eficácia.	Logs, tickets, atas, relatórios, contratos, testes, prints controlados.

3. Termos, Definições e Siglas

Termo/Sigla	Definição utilizada neste Manual
SGSI	Sistema de Gestão da Segurança da Informação.
SGI	Sistema de Gestão Integrado da 1 IT, abrangendo segurança, privacidade, anticorrupção/compliance e temas correlatos.
SGPI	Sistema de Gestão de Informações de Privacidade.
Ativo	Informação, dado, pessoa, processo, sistema, serviço, equipamento, instalação, contrato, conhecimento ou recurso com valor para a 1 IT.
CIA	Confidencialidade, Integridade e Disponibilidade.

Autenticidade	Propriedade de que uma entidade, usuário, origem ou registro é genuíno.
Rastreabilidade	Capacidade de reconstruir quem fez o quê, quando, onde, como e com qual resultado.
Risco	Efeito da incerteza sobre objetivos, expresso por cenário, impacto, probabilidade e controles.
Risco inerente	Risco antes da consideração dos controles existentes.
Risco residual	Risco remanescente após a implementação ou consideração dos controles.
Controle	Medida organizacional, de pessoas, física ou tecnológica que modifica ou mantém o risco.
SoA	Declaração de Aplicabilidade dos controles do Anexo A.
Incidente	Evento ou conjunto de eventos que compromete ou pode comprometer a segurança da informação.
Evento	Ocorrência observável em sistema, serviço, processo ou ambiente, ainda não classificada como incidente.
CSIRT	Equipe ou função de resposta a incidentes de segurança.
DPO/Encarregado	Pessoa indicada para atuar como canal de comunicação e apoiar a governança de proteção de dados pessoais.
IAM	Gestão de Identidades e Acessos.
JML	Joiner, Mover and Leaver - admissão, movimentação e desligamento.
PAM	Gestão de Acessos Privilegiados.
MFA	Autenticação multifator.
API	Interface de Programação de Aplicações.
SIEM	Gestão e correlação de eventos e informações de segurança.
EDR/XDR	Detecção e resposta em endpoints ou múltiplas camadas.
DLP	Prevenção de perda ou exfiltração de dados.
WAF	Firewall de Aplicação Web.
RTO	Tempo máximo objetivo para restabelecimento.
RPO	Ponto máximo de perda de dados aceitável.
BIA	Análise de Impacto nos Negócios.

BYOD	Uso autorizado de dispositivo pessoal para atividade corporativa.
Need-to-know	Acesso limitado a quem necessita da informação para executar atividade autorizada.
Least privilege	Menor privilégio necessário para a função e pelo menor período necessário.
Zero Trust	Abordagem de verificação contínua, sem confiança implícita baseada apenas em rede ou localização.
Segredo	Senha, token, chave, certificado privado, código de recuperação ou informação de autenticação equivalente.
Titular	Pessoa natural a quem os dados pessoais se referem.
Controlador	Agente que toma as decisões referentes ao tratamento de dados pessoais.
Operador/Processador	Agente que trata dados pessoais em nome do controlador e conforme instruções documentadas.
Suboperador	Terceiro contratado pelo operador para apoiar o tratamento de dados pessoais.

4. Contexto da Organização e do SGSI

4.1 Entendimento da organização e de seu contexto

A 1 IT deve manter análise documentada de questões internas e externas que possam afetar os resultados pretendidos do SGSI. A análise deve ser revista ao menos anualmente e quando ocorrer mudança relevante.

4.1.1 Questões externas

Dimensão	Questões a considerar	Evidência esperada
Legal e regulatória	LGPD, ANPD, Marco Civil, credenciamentos, portarias de órgãos de trânsito, requisitos de auditoria e preservação de registros.	Matriz de requisitos legais e regulatórios, pareceres e atualizações.
Clientes e mercado	Confidencialidade, disponibilidade, desempenho, rastreabilidade, integração, prazos e evidências.	Contratos, SLAs, atas, requisitos de segurança e pesquisas.

Tecnologia	Dependência de cloud/datacenter, APIs, certificados, internet, software de terceiros, atualizações e ameaças emergentes.	Arquitetura, inventário, análise de dependência, planos e testes.
Ameaças	Fraude, phishing, ransomware, exploração de APIs, credenciais comprometidas, erro de configuração, indisponibilidade e abuso interno.	Inteligência de ameaças, cenários de risco, varreduras e registros.
Terceiros	Provedores de nuvem, datacenter, telecom, desenvolvimento, suporte, segurança, certificados, e-mail e ferramentas SaaS.	Matriz de fornecedores, due diligence, contratos, evidências e monitoramento.
Clima e ambiente (Fatores Ambientais e sua análise de Impacto)	Eventos extremos que afetem energia, telecomunicações, deslocamento, fornecedores, instalações ou datacenters.	Avaliação de pertinência climática, BIA, continuidade e planos de contingência.

4.1.2 Questões internas

Dimensão	Questões a considerar	Evidência esperada
Estrutura	Organização simplificada, acumulação de funções e dependência de especialistas/terceiros.	Organograma, MA-001, RACI, substitutos e segregação compensatória.
Processos	Registro de contratos, integrações, suporte, atendimento, credenciamento, privacidade e fornecedores.	Mapa de processos, procedimentos, indicadores e donos.
Pessoas	Competência, treinamento, confidencialidade, cultura, trabalho remoto e desligamento.	Matriz de competências, EAD, avaliações e termos.
Tecnologia	Sistemas em implantação/operação, arquitetura distribuída, cloud/datacenter, redes, código, banco, logs e backup.	Inventário, diagramas, baselines, tickets e relatórios técnicos.

Governança	Primeiro ciclo de implantação e certificação, seis RNCs, necessidade de evidências e validação da SoA.	REL-AI-001, RNC-000, ATA-AC-001 e planos de ação.
Documentação	Uso do Outline Wiki e risco de divergência entre documento publicado e controle executado.	Lista mestra, versões, aprovações, permissões, logs e amostras de execução.

4.2 Partes interessadas e requisitos

Parte interessada	Necessidades e expectativas	Tratamento no SGSI
Clientes, credoras e parceiros	Confidencialidade, integridade, disponibilidade, SLA, rastreabilidade, segurança de integrações e resposta a incidentes.	Contratos, requisitos, criptografia, acesso, logs, continuidade e comunicação.
Órgãos de trânsito e reguladores	Conformidade, credenciamento, evidências, integridade de registros, disponibilidade e cooperação.	Matriz regulatória, trilhas, retenção, auditoria e gestão de mudanças.
Titulares de dados	Privacidade, transparência, segurança, direitos e resposta a incidentes.	MA-004, mapa de dados, AIPD/RIPD, canal, retenção e controles de acesso.
Colaboradores e prestadores	Regras claras, recursos seguros, treinamento e canais de reporte.	Integração, EAD, termos, suporte, IAM e processo disciplinar.
Fornecedores e suboperadores	Requisitos definidos, responsabilidades, SLAs, comunicação e critérios de avaliação.	RNC-001, contratos, due diligence, monitoramento e reversibilidade.
Alta Direção e sócios	Riscos conhecidos, continuidade, conformidade, indicadores e decisões fundamentadas.	Relatórios, análise crítica, auditoria, objetivos e planos de tratamento.
Auditores e certificadores	Evidências atuais, aprovadas, rastreáveis, eficazes e coerentes com a SoA.	Programa de auditoria, dossiê de evidências, amostragem e ações corretivas.

Sociedade e autoridades	Uso legítimo, proteção, cooperação, prevenção de ilícitos e respeito a direitos.	Compliance, segurança, privacidade, registros e comunicações formais.

4.3 Escopo formal do SGSI

> **Declaração de escopo:** O Sistema de Gestão da Segurança da Informação da 1 IT abrange os processos, pessoas, informações, aplicações, integrações, bancos de dados, serviços em nuvem/datacenter, infraestrutura de apoio, fornecedores críticos, documentos e atividades necessárias à operação tecnológica e à prestação de serviços relacionados ao registro de contratos de veículos, incluindo segurança, privacidade, suporte, atendimento, continuidade, desenvolvimento, mudanças e governança, na unidade administrativa e nos ambientes remotos e terceirizados autorizados.

O escopo deve ser mantido como informação documentada, aprovado pela Alta Direção e compatível com o escopo contratual, regulatório e de certificação.

4.4 Sistema de Gestão da Segurança da Informação

Macroprocesso	Entradas	Atividades	Saídas/Evidências
Governança	Contexto, partes interessadas, estratégia e requisitos.	Política, papéis, objetivos, comitê e análise crítica.	Manual, atas, decisões, recursos e comunicações.
Gestão de riscos	Processos, ativos, ameaças, vulnerabilidades e mudanças.	Identificação, análise, avaliação, tratamento e aceitação.	Matriz de riscos, PTR, SoA e aprovações.
Operação de controles	Riscos, requisitos e projetos.	Execução de controles organizacionais, humanos, físicos e tecnológicos.	Procedimentos, configurações, logs, tickets e relatórios.
Incidentes	Alertas, relatos, logs, reclamações e anomalias.	Triagem, contenção, investigação, recuperação e aprendizado.	Registro, linha do tempo, evidências, RCA e ações.
Continuidade	BIA, dependências, RTO/RPO e	Estratégia, planos, testes e	MA-005, testes, relatórios e

	cenários.	manutenção.	melhorias.
Avaliação e melhoria	Indicadores, auditoria, reclamações, incidentes e resultados.	Análise, auditoria, crítica, NC e melhoria.	REL-AI, ATA-AC, RNCs e planos de ação.

4.5 Processos terceirizados e responsabilidade compartilhada

A contratação de datacenter, nuvem, telecomunicações, desenvolvimento, suporte ou ferramenta de segurança não transfere à 1 IT a responsabilidade de definir requisitos, avaliar riscos, selecionar fornecedor, controlar acessos, acompanhar desempenho, gerir incidentes, manter evidências e planejar reversibilidade.

Os controles físicos e tecnológicos operados por provedores devem ser demonstrados por contratos, certificações, relatórios de auditoria, SLAs, evidências de configuração, testes, reuniões, incidentes e avaliações periódicas proporcionais ao risco.

5. Liderança, Política e Responsabilidades

5.1 Liderança e comprometimento

A Alta Direção deve:

- assegurar que a Política e os objetivos do SGSI sejam compatíveis com a estratégia e o contexto da 1 IT;
- integrar requisitos de segurança aos processos, contratos, projetos, aquisições, mudanças e decisões de negócio;
- prover recursos humanos, financeiros, tecnológicos e de tempo;
- apoiar os responsáveis por segurança e remover impedimentos;
- comunicar a importância da conformidade e do comportamento seguro;
- assegurar que o SGSI alcance resultados pretendidos;
- promover auditoria, análise crítica, correção e melhoria contínua;
- aprovar riscos residuais de alta criticidade e impedir aceitação informal de riscos críticos.

5.2 Política de Segurança da Informação

A Declaração Institucional apresentada no início deste Manual constitui a Política de Segurança da Informação da 1 IT. Seu desdobramento mínimo inclui:

- gestão baseada em riscos;

- menor privilégio e necessidade de conhecimento;
- classificação, rotulagem e tratamento da informação;
- segurança de pessoas antes, durante e após o vínculo;
- proteção de endpoints, redes, aplicações, APIs, bancos, nuvem e datacenters;
- criptografia e gestão de chaves/segredos;
- registro, monitoramento e preservação de evidências;
- backup, restauração, redundância e continuidade;
- prevenção, detecção e resposta a incidentes;
- segurança de fornecedores e cadeia de suprimentos;
- desenvolvimento seguro e gestão de mudanças;
- privacidade e proteção de dados pessoais;
- conformidade, auditoria e melhoria contínua.

A Política deve ser comunicada na admissão, disponibilizada no repositório oficial, reforçada em treinamento anual, incorporada a contratos relevantes e revisada no mínimo anualmente.

5.3 Estrutura de governança

Instância/Papel	Responsabilidades principais
Alta Direção	Aprovar política, escopo, objetivos, recursos, riscos residuais relevantes, mudanças críticas e análise crítica.
Comitê Multidisciplinar do SGI	Integrar Segurança, Privacidade, Compliance, Tecnologia, Operações, Jurídico e Continuidade; acompanhar riscos, indicadores, incidentes, auditorias e planos.
Responsável pelo SGSI	Coordenar o sistema, manter documentos e evidências, consolidar indicadores, riscos, SoA, auditorias e reporte à Direção.
Tecnologia/Segurança	Operar e evidenciar controles técnicos; manter arquitetura, IAM, logs, backup, hardening, vulnerabilidades, redes, cloud e incidentes.
Dono de processo	Definir requisitos, criticidade, controles, indicadores, continuidade e aceitação de risco do processo.
Dono de ativo/informação	Classificar, autorizar acesso, definir retenção, uso e descarte; revisar permissões.
Encarregado/DPO	Integrar segurança e privacidade; apoiar incidentes com dados pessoais, contratos, AIPD/RIPD, titulares e ANPD.

Jurídico/Compliance	Interpretar obrigações, revisar contratos, fornecedores, investigações, propriedade intelectual e comunicações formais.
RH/Administrativo	Aplicar controles de pessoas, admissão, mudança, desligamento, treinamento e disciplina.
Gestor de fornecedores	Inventariar, classificar, contratar, avaliar, monitorar e encerrar fornecedores de forma controlada.
Usuários	Cumprir políticas, proteger credenciais e ativos, participar de treinamentos e reportar eventos.

5.4 Matriz RACI essencial

Atividade	Alta Direção	Resp. SGSI	TI/Segurança	Operações	DPO	Jurídico/Comp
Aprovar Política e escopo	A	R	C	C	C	C
Avaliar e tratar riscos	A	R	C	C	C	C
Manter SoA	A	R	R	C	C	C
Criar/revogar acessos	I	C	R	C	I	I
Gerir mudanças	I/A quando crítica	C	R	C	C	C
Responder a incidentes	I/A quando crítico	R	R	C	R em dados pessoais	C
Avaliar fornecedores	I	C	C	C	C	R
Executar auditoria interna	I	R	C	C	C	C
Realizar análise crítica	A/R	C	C	C	C	C

Aceitar risco alto	A	R	C	C	C	C

Legenda: R = responsável por executar; A = autoridade final; C = consultado; I = informado.

5.5 Segregação e controles compensatórios

Em razão da estrutura simplificada, uma pessoa pode acumular funções desde que a combinação não crie conflito inaceitável. Devem ser utilizados controles compensatórios, como dupla aprovação, revisão independente, logs imutáveis, revisão posterior, limites de privilégio, rotação de responsabilidades e auditoria por amostragem.

6. Planejamento do SGSI

6.1 Ações para riscos e oportunidades

A 1 IT deve manter um processo único e integrado de riscos, atendendo ao plano de ação do RNC-002. O processo deve abranger segurança, privacidade, continuidade, integridade, fornecedores, tecnologia, pessoas e operação.

6.1.1 Metodologia de avaliação de riscos

1. definir processo, serviço, ativo, proprietário e contexto;
2. descrever cenário de risco com causa, evento e consequência;
3. identificar ameaças, vulnerabilidades, dependências e controles existentes;
4. avaliar impactos sobre confidencialidade, integridade, disponibilidade, privacidade, legal/regulatório, financeiro, operacional e reputacional;
5. avaliar probabilidade considerando exposição, histórico, capacidade do agente, facilidade de exploração e eficácia dos controles;
6. calcular o nível de risco inerente e residual;
7. comparar com critérios de aceitação;
8. selecionar tratamento, responsável, prazo, evidência e indicador;
9. aprovar o risco residual na alçada adequada;
10. monitorar e reavaliar em periodicidade definida ou após gatilho.

6.1.2 Escalas de impacto e probabilidade

Nota	Impacto	Critério de referência

1	Insignificante	Sem interrupção relevante, sem exposição significativa e correção rotineira.
2	Baixo	Impacto limitado, reversível, sem obrigação relevante de notificação.
3	Moderado	Afeta processo ou cliente, exige mobilização, pode gerar reclamação ou descumprimento menor.
4	Alto	Interrupção relevante, dados sensíveis, obrigação contratual/regulatória, perda financeira ou reputacional importante.
5	Crítico	Compromete serviço essencial, grande volume ou alta sensibilidade, risco a direitos, sanção grave, fraude relevante ou continuidade do negócio.

Nota	Probabilidade	Critério de referência
1	Rara	Exposição mínima, controles robustos, sem histórico e baixa capacidade de exploração.
2	Improvável	Pode ocorrer em condições incomuns.
3	Possível	Cenário plausível, com exposição e controles moderados.
4	Provável	Histórico, vulnerabilidade conhecida ou alta exposição.
5	Quase certa	Ocorrência esperada ou em curso, controles insuficientes ou exploração simples.

Nível de risco = Impacto x Probabilidade.

Faixa	Classificação	Tratamento e alçada
1 a 4	Baixo	Pode ser aceito pelo dono do processo, com registro e revisão.
5 a 9	Médio	Requer monitoramento e tratamento proporcional aprovado pelo responsável do SGSI e dono do processo.
10 a 16	Alto	Exige plano formal, prazo, responsável e aprovação da Alta Direção para risco residual.
17 a 25	Crítico	Não deve ser aceito como condição permanente; requer ação imediata, escalonamento e decisão da Alta Direção.

6.1.3 Opções de tratamento

- **Modificar/Mitigar:** implementar ou fortalecer controles;
- **Evitar:** interromper atividade, tecnologia, acesso ou prática de risco inaceitável;

- **Compartilhar/Transferir:** contratar seguro, fornecedor ou acordo, sem eliminar a responsabilidade de governança;
- **Aceitar:** decisão formal baseada em justificativa, prazo de revisão e alçada;
- **Explorar oportunidade:** adotar melhoria que reduza risco ou aumente resiliência e confiança.

6.1.4 Declaração de Aplicabilidade - SoA

A SoA deve conter todos os controles do Anexo A da ISO/IEC 27001:2022, justificativa de inclusão ou exclusão, status, responsável, documentos, evidências e vínculo com riscos. A exclusão de controle deve ser excepcional, tecnicamente fundamentada e não pode comprometer atendimento de requisito legal, contratual ou risco identificado.

O RNC-005 deve ser encerrado somente após validação técnica documentada dos controles de redes, arquitetura, cloud/datacenter, autenticação, logs, monitoramento, criptografia, desenvolvimento, segregação e continuidade.

6.2 Objetivos de segurança da informação

Objetivo	Indicador	Meta institucional inicial	Frequência	Responsável
Concluir capacitação obrigatória	% de público-alvo com EAD, avaliação e termo concluídos	100% antes da Fase 2 e >= 95% nos ciclos regulares	Mensal/Anual	RH + SGSI
Revisar acessos críticos	% de acessos privilegiados e sensíveis revisados	100% no período definido	Mensal/Trimestral	TI + Donos
Corrigir vulnerabilidades	% de vulnerabilidades críticas/altas tratadas no SLA	>= 95%, sem crítica vencida sem exceção aprovada	Mensal	TI/Segurança
Testar restauração	% de testes de backup executados com sucesso	100% do plano anual	Mensal/Trimestral	TI
Avaliar fornecedores	% de fornecedores	100%	Trimestral/Anual	Jurídico + SGSI

críticos	críticos avaliados e contratualmente adequados			
Registrar mudanças	% de mudanças relevantes com ticket, risco, teste, aprovação e rollback	100%	Mensal	TI/Operações
Melhorar resposta a incidentes	Tempo de detecção, reconhecimento, contenção e recuperação	Tendência de redução e cumprimento dos SLAs	Mensal/Por incidente	CSIRT
Manter documentos controlados	% de documentos críticos com versão, aprovação e revisão válida	100%	Trimestral	SGSI
Encerrar ações corretivas	% de RNCs no prazo e com eficácia verificada	100% das críticas; >= 90% geral	Mensal	SGSI + responsáveis

Os objetivos devem possuir plano de ação, recursos, responsáveis, prazo, forma de medição e avaliação de resultado.

6.3 Planejamento de mudanças

Mudanças em sistemas, integrações, APIs, infraestrutura, serviços em nuvem, fornecedores, acessos, criptografia, classificação, retenção, arquitetura, processos ou documentos críticos devem ser planejadas.

O registro mínimo inclui: solicitante, justificativa, escopo, ativos, impacto, risco, dependências, dados pessoais, segurança, continuidade, testes, homologação, janela, comunicação, aprovação, plano de rollback, evidência de execução e validação pós-mudança. O processo deve atender ao RNC-004.

7. Apoio

7.1 Recursos

A 1 IT deve prover recursos compatíveis com os riscos e com a criticidade de seus serviços. A terceirização pode suprir capacidade técnica, desde que existam contrato, responsabilidades, SLA, evidências, supervisão e contingência.

Recursos mínimos incluem: responsável pelo SGSI e substituto; donos de processo e ativos; ferramenta de chamados; proteção de endpoints; controle de acesso; logs; backup; varredura de vulnerabilidades; monitoramento; repositório controlado; orçamento para correções, testes e capacitação.

7.2 Competência

A competência deve ser definida por função e demonstrada por formação, experiência, treinamento, avaliação ou certificação. Lacunas devem gerar plano de capacitação ou contratação de apoio especializado.

Perfil	Competências mínimas	Evidências
Alta Direção	Governança, riscos, responsabilidades, análise crítica e priorização.	Treinamento executivo, atas e decisões.
Responsável SGSI	ISO/IEC 27001, riscos, SoA, auditoria, indicadores e melhoria.	Currículo, cursos, certificados e atuação.
TI/Segurança	IAM, redes, cloud, hardening, logs, backup, vulnerabilidades, incidentes e mudanças.	Trilhas, relatórios e amostras técnicas.
Desenvolvimento	SDLC seguro, revisão de código, testes, segredos, dependências e APIs.	Treinamentos, repositórios, pipelines e relatórios.
Operações/Atendimento	Uso seguro, classificação, privacidade, fraude e reporte de eventos.	EAD, avaliação e termos.
DPO/Privacidade	LGPD, riscos, incidentes, direitos, contratos e AIPD/RIPD.	Nomeação, qualificação e pareceres.
Auditores	Norma, técnicas de auditoria, imparcialidade e análise de evidências.	AV-AUD-001, plano e registros.

7.3 Conscientização e treinamento

Todos devem concluir treinamento inicial antes ou imediatamente após obter acesso e reciclagem anual em EAD. Conteúdo mínimo:

- política, responsabilidades e consequências;
- classificação e tratamento da informação;
- senhas, MFA, phishing, engenharia social e fraude;
- trabalho remoto, dispositivos e uso aceitável;
- proteção de dados pessoais e canais do DPO;
- reporte de eventos e incidentes;
- segurança de fornecedores e compartilhamento;
- continuidade e procedimentos de emergência;
- temas específicos por função, como desenvolvimento seguro, IAM, logs e investigação.

O RNC-006 somente deve ser encerrado com lista de público-alvo, conclusão, avaliação, aceite de termos, tratamento de pendências e verificação de eficácia.

7.4 Comunicação

Comunicação	Conteúdo	Público	Canal	Frequênci
Política e mudanças	Versão vigente e alterações relevantes	Todos	Outline, EAD, e-mail	Anual e po mudança
Alertas	Phishing, vulnerabilidades, campanhas e lições	Usuários afetados	E-mail, mensageria, portal	Conforme
Incidentes críticos	Situação, impacto, ação e orientação	Direção e áreas autorizadas	Canal restrito	Imediato
Clientes/Reguladores	Notificação contratual ou legal	Parte definida	Canal formal	Conforme
Fornecedores	Requisitos, falhas, mudanças e avaliações	Fornecedores críticos	Contrato, ticket, reunião	Contrataçã revisão

Nenhuma pessoa não autorizada pode falar em nome da 1 IT sobre incidente, vulnerabilidade, investigação, cliente, dado pessoal ou arquitetura.

7.5 Informação documentada

7.5.1 Criação e atualização

Todo documento deve possuir título, código, versão, data, classificação, elaborador, revisor/aprovador, proprietário, periodicidade de revisão e histórico de alterações. Conteúdo técnico deve ser validado pela área responsável.

7.5.2 Controle no Outline Wiki

O Outline Wiki deve ser tratado como ativo crítico e controlado, no mínimo, por:

- MFA ou SSO forte para contas administrativas e usuários, quando disponível;
- menor privilégio por coleção, grupo e documento;
- revisão periódica de administradores, membros, convidados e compartilhamentos;
- compartilhamento público desabilitado por padrão e autorizado somente mediante avaliação;
- classificação e segregação de documentos sensíveis;
- trilhas de auditoria, versionamento e registro de alterações;
- backup/exportação e teste de restauração do conteúdo e metadados;
- atualização de plataforma, dependências, banco, cache, proxy e componentes;
- proteção de chaves de API, integrações, webhooks e contas de serviço;
- procedimento de admissão, mudança e desligamento;
- controle de anexos, dados pessoais, contratos, denúncias e evidências técnicas;
- plano de continuidade e contingência para indisponibilidade do repositório.

7.5.3 Retenção e descarte

A retenção deve considerar finalidade, lei, contrato, defesa de direitos, auditoria, credenciamento, prazo prescricional e minimização. O descarte deve ser autorizado, rastreável e seguro, incluindo cópias, backups e mídias quando tecnicamente possível.

8. Operação e Controles do SGSI

8.1 Planejamento e controle operacional

Os processos devem possuir critérios, responsáveis, entradas, saídas, registros, controles e indicadores. Mudanças e processos terceirizados devem ser controlados. Evidências devem demonstrar execução, e não apenas intenção documental.

8.2 Avaliação de riscos durante a operação

A avaliação de riscos deve ser repetida ao menos anualmente e quando houver novo produto, integração, fornecedor, tecnologia, incidente relevante, mudança regulatória,

alteração de dados pessoais, expansão geográfica, mudança de arquitetura ou desvio significativo.

8.3 Tratamento de riscos

O Plano de Tratamento de Riscos deve identificar risco, controle, ação, responsável, prazo, recurso, indicador, evidência, risco residual e aprovação. A eficácia deve ser verificada após implantação.

8.4 Inventário e propriedade de ativos

Todos os ativos relevantes devem constar em inventário com proprietário, custodiante, localização, fornecedor, ambiente, criticidade, classificação, dependências, backup, retenção, fim de vida e vínculo com processos. Ativos sem proprietário não devem permanecer em produção.

8.5 Classificação e tratamento da informação

8.5.1 Níveis de classificação

Nível	Critério	Exemplos	Regras mínimas
Público	Divulgação autorizada sem dano relevante.	Conteúdo institucional aprovado, materiais públicos.	Aprovação de comunicação; integridade e versão controladas.
Uso Interno	Uso de colaboradores e terceiros autorizados; divulgação externa indevida gera impacto limitado.	Procedimentos gerais, organogramas, comunicados internos.	Acesso autenticado; envio apenas por canais corporativos.
Confidencial	Divulgação indevida pode causar dano relevante a clientes, titulares, contratos, operação ou reputação.	Contratos, dados de clientes, relatórios, arquitetura, riscos, logs.	Need-to-know, criptografia em trânsito, acesso registrado, compartilhamento controlado.
Restrito	Informação crítica cuja exposição pode causar incidente grave, fraude, comprometimento ou	Senhas, chaves, tokens, dados sensíveis, vulnerabilidades	Cofre de segredos, acesso nominal e temporário, MFA, logs, criptografia e

	obrigação de notificação.	exploráveis, investigações.	proibição de canais comuns.

8.5.2 Regras de manuseio

O proprietário define classificação. O usuário mantém a classificação em cópias, anexos, exportações e comunicações. Reclassificação e desclassificação exigem avaliação e registro. Informações confidenciais ou restritas não podem ser inseridas em ferramentas não aprovadas, incluindo serviços pessoais e sistemas públicos de inteligência artificial.

8.6 Gestão de identidades e acessos

- contas individuais e identificáveis; contas compartilhadas somente por exceção aprovada e com rastreabilidade compensatória;
- MFA para acessos administrativos, remotos, cloud, código, Outline e sistemas críticos;
- acesso por função, menor privilégio e necessidade de conhecimento;
- fluxo JML com aprovação do dono do ativo;
- revogação imediata no desligamento ou perda de necessidade;
- revisão periódica de acessos comuns, privilegiados e contas técnicas;
- PAM, cofre de senhas ou mecanismo equivalente para privilégios críticos;
- proibição de reutilização e compartilhamento de credenciais;
- segregação entre administração, operação, desenvolvimento e auditoria quando possível;
- registro e investigação de falhas repetidas de autenticação e uso anômalo.

8.7 Criptografia e gestão de chaves/segredos

Dados confidenciais ou restritos devem utilizar criptografia adequada em trânsito e, quando aplicável, em repouso. Algoritmos, protocolos e tamanhos de chave devem seguir padrões atuais e configurações aprovadas.

Chaves e segredos devem possuir proprietário, finalidade, ambiente, validade, controle de acesso, rotação, backup seguro quando necessário, revogação e descarte. Segredos não podem ser armazenados em código-fonte, arquivos públicos, wiki, e-mail ou mensageria sem proteção.

8.8 Segurança de endpoints e dispositivos

Endpoints corporativos devem possuir inventário, configuração segura, bloqueio de tela, atualização, antimalware/EDR, criptografia quando aplicável, firewall, restrição de privilégios, backup de dados autorizados e capacidade de resposta. Dispositivos perdidos ou roubados devem ser reportados imediatamente.

BYOD depende de autorização, termo, requisitos técnicos, segregação de dados, proteção, capacidade de remoção corporativa e avaliação de privacidade.

8.9 Redes, arquitetura, cloud e datacenters

A arquitetura deve ser documentada, aprovada e revisada. Devem ser aplicados, conforme risco:

- segmentação de ambientes e redes;
- firewalls, WAF, filtros e regras mínimas;
- acesso administrativo por canais seguros;
- proteção de APIs e limitação de taxa;
- gestão de certificados e DNS;
- criptografia de comunicações;
- redundância, disponibilidade e monitoramento;
- configuração segura e infraestrutura como código, quando aplicável;
- registros de alteração e revisão de regras;
- validação de responsabilidade compartilhada com cloud/datacenter;
- evidências de Tier, certificações, continuidade, segurança física e testes dos provedores.

Como a sede administrativa não concentra infraestrutura crítica, controles físicos e ambientais de datacenter devem ser exigidos e monitorados nos provedores, enquanto a unidade local deve manter controles proporcionais para recepção, estações, documentos e conectividade.

8.10 Logs, monitoramento e sincronização de tempo

Sistemas críticos devem registrar autenticação, privilégios, alterações, transações, erros, eventos de segurança, integrações, ações administrativas e acessos a dados relevantes. Logs devem ser protegidos contra alteração, possuir retenção definida, acesso restrito e horário sincronizado.

Alertas devem possuir responsável, criticidade, canal, SLA, procedimento de triagem e registro de decisão. Ausência de alerta não comprova ausência de incidente; a cobertura e eficácia do monitoramento devem ser testadas.

8.11 Gestão de vulnerabilidades, patching e hardening

- inventário de tecnologias e versões;
- fontes de alerta e inteligência de vulnerabilidades;
- varreduras autenticadas e não autenticadas conforme risco;
- classificação por criticidade, exposição e contexto;

- SLA de correção e exceção formal;
- testes antes da implantação e validação após correção;
- baseline de configuração segura para sistemas, redes, cloud, bancos e aplicações;
- revisão de desvios e remoção de serviços, portas, contas e componentes desnecessários;
- teste de invasão proporcional e autorizado, com escopo, regras, evidências e remediação.

8.12 Proteção contra malware, phishing e conteúdo malicioso

A 1 IT deve manter proteção técnica, filtragem, atualização, bloqueio de execução indevida, restrição de macros, treinamento, simulações e resposta. Suspeitas de phishing devem ser reportadas sem interação adicional com o conteúdo.

8.13 Backup, restauração e redundância

Backups devem considerar criticidade, RPO, RTO, retenção, criptografia, segregação, imutabilidade quando aplicável, cópia externa e capacidade de restauração. O princípio 3-2-1-1-0 pode ser adotado conforme risco: três cópias, dois meios, uma externa, uma imutável/offline e zero erros após verificação.

Testes de restauração devem ser planejados, registrados e avaliados. Ter backup sem teste de recuperação não é evidência suficiente de continuidade.

8.14 Continuidade e prontidão de TIC

O MA-005 deve definir BIA, processos críticos, dependências, RTO/RPO, estratégias, contatos, comunicação, contingência, retorno e testes. Cenários devem incluir indisponibilidade de cloud/datacenter, falha de integração, comprometimento de credenciais, ransomware, perda de conectividade, indisponibilidade de fornecedor e evento climático relevante.

8.15 Gestão de eventos e incidentes

8.15.1 Fluxo mínimo

1. detectar ou receber relato;
2. registrar data, fonte, ativo, evidências e impacto inicial;
3. classificar evento/incidente e severidade;
4. preservar evidências e limitar divulgação;
5. conter, erradicar e recuperar;
6. comunicar partes internas e externas conforme alçada;
7. analisar causa raiz e extensão;

8. executar ações corretivas;
9. registrar lições aprendidas e atualizar riscos, controles e documentos;
10. verificar eficácia e encerrar formalmente.

8.15.2 Severidade e metas preliminares

Nível	Exemplo	Reconhecimento inicial	Escalonamento
S1 - Crítico	Indisponibilidade ampla, exfiltração relevante, ransomware, fraude grave, credencial administrativa comprometida.	Até 15 minutos, quando monitorado 24x7, ou imediatamente após ciência.	Alta Direção, SGSI, TI, DPO/Jurídico conforme impacto.
S2 - Alto	Comprometimento limitado de serviço crítico, vulnerabilidade explorada, dados confidenciais expostos.	Até 1 hora.	Gestores e funções especializadas.
S3 - Médio	Evento controlado com impacto moderado e sem propagação.	Até 4 horas úteis.	Responsável do processo e SGSI.
S4 - Baixo	Alerta sem impacto confirmado ou evento rotineiro.	Até 1 dia útil.	Tratamento operacional e monitoramento.

Metas devem ser ajustadas a contratos, cobertura de suporte e capacidade real, aprovadas pela Direção e testadas.

8.16 Incidentes com dados pessoais

O DPO deve ser envolvido quando houver dados pessoais. A organização deve avaliar natureza, categoria, volume, titulares, consequências, medidas, risco ou dano relevante, papel como controladora ou operadora e deveres de comunicação. Quando atuar como operadora, deve informar o controlador sem demora injustificada e cooperar conforme contrato e lei.

Comunicações à ANPD, titulares, clientes ou autoridades devem ser aprovadas e registradas, observando a regulamentação vigente.

8.17 Segurança de fornecedores e cadeia de suprimentos

O processo deve atender ao RNC-001 e incluir:

- inventário, serviço, dados, acessos, localização e dependências;

- classificação de criticidade;
- due diligence inicial e periódica;
- requisitos de segurança, privacidade, continuidade, compliance e subcontratação;
- SLA, notificação de incidentes, direito de auditoria e fornecimento de evidências;
- controle de mudanças e vulnerabilidades;
- retorno, eliminação, portabilidade e reversibilidade no encerramento;
- monitoramento de desempenho e risco;
- plano de substituição ou contingência.

8.18 Desenvolvimento seguro e segurança de aplicações/APIs

A segurança deve integrar requisitos, arquitetura, design, codificação, revisão, teste, implantação, operação e descontinuação. Devem ser considerados:

- requisitos de autenticação, autorização, sessão, criptografia, logging, privacidade e disponibilidade;
- segregação de desenvolvimento, homologação e produção;
- revisão de código e proteção do repositório;
- análise de dependências, componentes e licenças;
- SAST, DAST, SCA, testes de API e teste manual conforme criticidade;
- gestão de segredos e assinatura de artefatos;
- dados de teste anonimizados, mascarados ou sintéticos;
- controle de pipelines e mudanças;
- correção de vulnerabilidades antes da produção ou exceção formal;
- monitoramento pós-implantação e plano de rollback.

8.19 Transferência de informações e integrações

Transferências devem possuir finalidade, base/autorização, origem, destino, classificação, canal, criptografia, autenticação, integridade, logs, retenção, descarte e responsável. APIs devem aplicar autenticação forte, autorização por escopo, validação de entrada, proteção contra abuso, limitação de taxa, gestão de erros e monitoramento.

8.20 Trabalho remoto

O trabalho remoto deve utilizar dispositivos e acessos autorizados, MFA, VPN/Zero Trust quando aplicável, ambiente privado, proteção de tela, proibição de terceiros, armazenamento corporativo, atualização e reporte imediato de eventos. Documentos físicos confidenciais devem ser evitados e, quando necessários, protegidos e devolvidos/destruídos com registro.

8.21 Segurança física e ambiental

Na sede administrativa devem existir controle de acesso proporcional, acompanhamento de visitantes, proteção de estações e documentos, mesa e tela limpas, prevenção contra furto, incêndio, água, energia e outras ameaças. Equipamentos não devem ficar acessíveis ao público sem supervisão.

Nos datacenters e instalações de fornecedores, os controles devem ser comprovados por contratos, certificações, relatórios, auditorias e avaliações. A 1 IT deve conhecer localização, redundância, acesso, monitoramento, manutenção, descarte e continuidade dos ativos relevantes.

8.22 Mídias, descarte e reutilização

O uso de mídia removível deve ser restrito e autorizado. Informações devem ser apagadas de forma segura antes de descarte, devolução ou reutilização de equipamentos e mídias. Quando a eliminação completa não for tecnicamente possível, devem ser aplicados controles de criptografia, expiração, segregação e retenção documentada.

8.23 Uso aceitável

É proibido:

- compartilhar credenciais, burlar controles ou usar privilégios sem finalidade;
- instalar software, extensão ou serviço não autorizado;
- armazenar informação corporativa em contas ou dispositivos pessoais sem autorização;
- desativar proteção, logs, criptografia ou atualização;
- executar teste, varredura, exploração ou coleta sem autorização formal;
- enviar dados confidenciais a ferramentas públicas de IA, e-mail pessoal ou mensageria não aprovada;
- acessar conteúdo ilegal, ofensivo ou incompatível com a atividade;
- utilizar ativos para fraude, assédio, violação de direitos ou atividade ilícita.

8.24 Gestão de evidências

Evidências devem ser autênticas, íntegras, datadas, rastreáveis e protegidas. Prints isolados devem ser complementados por fonte, contexto, responsável, período e método de coleta. Para incidentes e investigações, deve existir cadeia de custódia proporcional.

9. Avaliação de Desempenho

9.1 Monitoramento, medição, análise e avaliação

A 1 IT deve definir o que medir, método, frequência, responsável, meta, fonte, retenção e forma de análise. Indicadores devem apoiar decisões e não ser utilizados para ocultar ausência de dados ou de controles.

Indicadores mínimos: riscos altos/críticos; vulnerabilidades; incidentes; disponibilidade; backup/restauração; acessos; mudanças; fornecedores; treinamento; documentos vencidos; ações corretivas; direitos de titulares; testes de continuidade; auditorias.

9.2 Auditoria interna

Auditorias devem ser planejadas considerando importância, riscos, mudanças e resultados anteriores. Auditores devem possuir competência e independência, conforme AV-AUD-001. O programa deve registrar critérios, escopo, método, amostra, achados, evidências, responsáveis, prazos e acompanhamento.

O PA-AI-001 e o REL-AI-001 integram o primeiro ciclo. A auditoria deve verificar não apenas a existência de documentos, mas a implantação e eficácia por meio de logs, tickets, configurações, contratos, entrevistas, testes e amostras.

9.3 Análise crítica pela Direção

A análise crítica deve ocorrer ao menos anualmente e incluir:

- situação das ações anteriores;
- mudanças internas e externas, inclusive clima quando pertinente;
- necessidades de partes interessadas;
- desempenho de objetivos, indicadores, incidentes, não conformidades e auditorias;
- riscos, SoA, fornecedores, recursos e oportunidades;
- adequação de política e escopo;
- decisões sobre melhoria, mudanças e recursos.

A ATA-AC-001 deve ser mantida com participantes, evidências, decisões, responsáveis, prazos, aprovação e acompanhamento de eficácia.

10. Melhoria

10.1 Não conformidade e ação corretiva

Quando ocorrer não conformidade, a 1 IT deve:

1. reagir, controlar e corrigir;
2. tratar consequências;

3. avaliar necessidade de eliminar causa;
4. investigar causa raiz com método adequado;
5. verificar ocorrências semelhantes ou potenciais;
6. planejar e implementar ação corretiva;
7. atualizar riscos, SoA, documentos e controles;
8. verificar eficácia;
9. encerrar com aprovação independente da execução, quando possível.

10.2 Melhoria contínua

Fontes de melhoria incluem incidentes, alertas, testes, auditorias, sugestões, reclamações, análise crítica, ameaças, mudanças, indicadores, fornecedores e lições aprendidas. O responsável pelo SGSI deve manter backlog priorizado, com valor, risco, responsável, prazo e resultado.

10.3 Prioridades de prontidão e fechamento

Referência	Prioridade desta revisão	Evidência de fechamento esperada
RNC-001	Formalizar e avaliar fornecedores críticos.	Matriz, contratos, avaliações, SLAs, monitoramento e eficácia.
RNC-002	Consolidar riscos em matriz única.	Metodologia, registros, PTR, riscos residuais e aprovações.
RNC-003	Comprovar análise crítica real.	Convite, participantes, entradas, decisões, assinaturas e acompanhamento.
RNC-004	Institucionalizar mudanças.	Tickets/PMUD, impacto, testes, aprovação, rollback e validação.
RNC-005	Finalizar SoA e evidências técnicas.	Arquitetura, redes, cloud, logs, hardening, vulnerabilidades, criptografia e testes.
RNC-006	Concluir EAD e termos.	Público-alvo, conclusão, avaliação, ciência e verificação de eficácia.

11. Cumprimento, Exceções e Vigência

11.1 Cumprimento e medidas

Violações devem ser registradas e avaliadas com proporcionalidade, imparcialidade, confidencialidade e respeito às regras trabalhistas, contratuais e legais. Medidas podem incluir orientação, treinamento, advertência, suspensão de acesso, ação disciplinar, rescisão, reparação e comunicação a autoridade.

11.2 Exceções

Exceções devem conter requisito, justificativa, risco, controles compensatórios, responsável, prazo, aprovação e revisão. Exceção sem data de expiração é proibida, salvo decisão formal da Alta Direção com revisão periódica.

11.3 Revisão e vigência

Este Manual entra em vigor após aprovação da Alta Direção e substitui a versão anterior do MA-002. Deve ser revisto anualmente ou antes, em caso de mudança relevante, incidente, auditoria, nova obrigação, alteração de escopo, fornecedor crítico, arquitetura, tecnologia ou processo.

Anexo A - Modelos Operacionais

A.1 Registro mínimo de risco

Campo	Conteúdo esperado
ID e data	Identificador, versão e data de avaliação.
Processo/ativo	Processo, serviço, sistema, dado, fornecedor ou local.
Proprietário	Dono do processo/risco e responsáveis consultados.
Cenário	Causa, evento e consequência.
Segurança	Impactos em confidencialidade, integridade, disponibilidade, autenticidade e rastreabilidade.
Privacidade/legal	Dados pessoais, titulares, obrigação, contrato e sanção.
Controles existentes	Controles e evidências atuais.
Risco inerente	Impacto, probabilidade e nível antes dos controles.
Risco residual	Impacto, probabilidade e nível após controles.
Tratamento	Ação, controle, responsável, prazo, recurso e evidência.
Aceitação	Alçada, justificativa, data e prazo de revisão.

A.2 Registro mínimo de incidente

Campo	Conteúdo esperado

Identificação	ID, data/hora, relator, canal e ativo.
Classificação	Evento/incidente, categoria e severidade.
Escopo	Sistemas, dados, usuários, clientes, fornecedores e localidades.
Linha do tempo	Detecção, comunicação, decisões, contenção, recuperação e encerramento.
Evidências	Logs, imagens, arquivos, hashes, tickets, e-mails e cadeia de custódia.
Impacto	CIA, privacidade, legal, contratual, financeiro, operacional e reputacional.
Resposta	Contenção, erradicação, recuperação e validação.
Comunicação	Interna, clientes, controladores, titulares, ANPD e outras autoridades.
Causa e ações	RCA, correção, ação corretiva, responsável, prazo e eficácia.
Aprendizado	Riscos, SoA, procedimentos, treinamento e indicadores atualizados.

A.3 Checklist de mudança

- ☐ Solicitação e justificativa registradas.
- ☐ Escopo, ativos, ambientes e responsáveis identificados.
- ☐ Risco de segurança, privacidade e continuidade avaliado.
- ☐ Dependências, fornecedores e requisitos contratuais considerados.
- ☐ Testes, homologação e critérios de aceite definidos.
- ☐ Backup ou ponto de retorno disponível, quando aplicável.
- ☐ Plano de rollback validado.
- ☐ Aprovação pela alçada competente.
- ☐ Comunicação às partes afetadas.
- ☐ Implementação registrada.
- ☐ Validação pós-mudança e monitoramento concluídos.
- ☐ Documentos, inventário, riscos e SoA atualizados.

A.4 Checklist de publicação no Outline Wiki

- ☐ Código, título, versão, data e classificação conferidos.
- ☐ Elaborador, revisor, aprovador e proprietário definidos.
- ☐ Referências e links internos validados.

- [ ] Ausência de senhas, tokens, chaves e segredos confirmada.
- [ ] Dados pessoais e informações sensíveis minimizados.
- [ ] Permissão da coleção/documento revisada.
- [ ] Compartilhamento público desabilitado ou formalmente aprovado.
- [ ] Conteúdo técnico validado pela área responsável.
- [ ] Histórico de alterações preenchido.
- [ ] Documento anterior arquivado/substituído sem perda de rastreabilidade.
- [ ] Prazo de revisão e responsável por atualização definidos.

Anexo B - Matriz de Atendimento aos Requisitos da ISO/IEC 27001:2022

> **Nota:** as descrições abaixo são paráfrases operacionais e não reproduzem o texto integral da norma. A confirmação de conformidade exige consulta à norma oficial, à SoA, aos riscos e às evidências vigentes.

Tópico	Descrição operacional	Aplicável	Justificativa de atendimento	Documentos e evidências de referência
4.1	Identificar e revisar questões internas e externas que afetem os resultados do SGSI, incluindo a pertinência de mudanças climáticas.	Sim	O negócio depende de regulação, tecnologia, terceiros, cloud/datacenter, pessoas e continuidade.	MA-002 seção 4; matriz de contexto; BIA; ATA-AC-001.
4.2	Determinar partes interessadas, requisitos pertinentes e quais requisitos serão tratados pelo SGSI.	Sim	Clientes, órgãos de trânsito, titulares, fornecedores e auditores possuem requisitos de segurança.	Matriz de partes interessadas; contratos; requisitos legais; MA-004.
4.3	Definir limites, interfaces e	Sim	É necessário delimitar	Declaração de escopo; mapa de

	aplicabilidade do escopo do SGSI.		processos de registro, tecnologia, terceiros, unidade e ambientes remotos.	processos; inventários; contratos.
4.4	Estabelecer, implementar, manter e melhorar o SGSI e seus processos.	Sim	O SGSI é base do ciclo de certificação e da governança da 1 IT.	MA-002; PO-010; indicadores; auditorias; ATA-AC-001.
5.1	Demonstrar liderança, integração ao negócio, recursos, comunicação e apoio à melhoria.	Sim	Controles dependem de prioridade, alçada e recursos da Alta Direção.	Política; atas; orçamento; decisões; análise crítica.
5.2	Estabelecer e comunicar política adequada, com compromisso de requisitos e melhoria.	Sim	A política é necessária para orientar pessoas e controles.	Declaração Institucional; EAD; comunicações; termos.
5.3	Atribuir e comunicar papéis, responsabilidades e autoridades.	Sim	A estrutura simplificada exige clareza e controles compensatórios.	MA-001; RACI; nomeações; contratos.
6.1.1	Planejar ações para riscos e oportunidades e integrá-las aos processos.	Sim	O primeiro ciclo possui RNCs e riscos transversais a tratar.	Matriz de riscos; RNC-002; PTR; planos.
6.1.2	Definir e aplicar processo consistente de avaliação de riscos de segurança.	Sim	Riscos de APIs, cloud, credenciais, dados e terceiros devem ser comparáveis e auditáveis.	PO-004; metodologia 5x5; registros de risco.

6.1.3	Tratar riscos, selecionar controles, manter SoA, aprovar plano e risco residual.	Sim	A SoA e as evidências técnicas são prioridade do RNC-005.	SoA; PTR; aprovações; matriz Anexo C.
6.2	Definir objetivos coerentes, mensuráveis, monitorados, comunicados e atualizados.	Sim	Objetivos permitem demonstrar desempenho e eficácia.	Tabela de objetivos; indicadores; relatórios.
6.3	Planejar mudanças do SGSI de forma controlada.	Sim	Sistemas e integrações em implantação exigem formalização, conforme RNC-004.	PO-007; tickets/PMUD; testes; rollback.
7.1	Determinar e prover recursos necessários.	Sim	A operação depende de equipe, fornecedores, ferramentas e orçamento.	Plano de recursos; contratos; orçamento; atas.
7.2	Assegurar competência e reter evidências.	Sim	Papéis técnicos, DPO, gestores e auditores exigem capacitação.	Matriz de competências; AV-AUD-001; certificados.
7.3	Assegurar conscientização sobre política, contribuição e consequências.	Sim	RNC-006 exige EAD e termos antes da Fase 2.	PO-009; EAD; avaliações; aceites.
7.4	Planejar comunicações internas e externas.	Sim	Incidentes, clientes, reguladores e fornecedores requerem comunicação controlada.	Plano de comunicação; templates; protocolos.

7.5.1	Manter informação documentada requerida e necessária.	Sim	O Outline é repositório central e deve refletir controles reais.	Lista mestra; MA/PO/IT/FO; evidências.
7.5.2	Controlar identificação, formato, revisão e aprovação na criação/atualização.	Sim	Versões inconsistentes comprometem auditoria e operação.	PO-001/PO-013; histórico; aprovações.
7.5.3	Controlar acesso, distribuição, armazenamento, preservação, retenção e descarte.	Sim	Documentos incluem riscos, contratos, dados e evidências sensíveis.	Permissões Outline; backups; matriz de retenção.
8.1	Planejar, executar e controlar processos, mudanças e terceiros.	Sim	A eficácia do SGSI depende de execução rotineira e rastreável.	Procedimentos, tickets, contratos, logs e checklists.
8.2	Realizar avaliações de risco em intervalos e após mudanças significativas.	Sim	A exposição muda com sistemas, integrações, fornecedores e regulação.	Calendário de riscos; avaliações por mudança.
8.3	Implementar o plano de tratamento e reter resultados.	Sim	Ações precisam de evidência e eficácia, não apenas planejamento.	PTR; tickets; relatórios; validação.
9.1	Definir monitoramento, medição, análise e avaliação do SGSI.	Sim	Indicadores suportam decisões, auditoria e melhoria.	Painel de indicadores; relatórios; atas.
9.2.1	Realizar auditorias internas planejadas para avaliar conformidade e implementação.	Sim	A certificação exige auditoria interna efetiva.	PA-AI-001; REL-AI-001; evidências.

9.2.2	Manter programa, critérios, escopo, imparcialidade, resultados e correções.	Sim	É necessário acompanhar achados e evitar conflito de interesse.	Programa; AV-AUD-001; RNCs; follow-up.
9.3.1	Realizar análise crítica em intervalos planejados.	Sim	A Alta Direção deve avaliar adequação, suficiência e eficácia.	ATA-AC-001; agenda; participantes.
9.3.2	Avaliar entradas como mudanças, desempenho, auditorias, riscos e oportunidades.	Sim	O primeiro ciclo requer consolidação de dados e decisões.	Indicadores; riscos; auditorias; incidentes.
9.3.3	Registrar decisões sobre melhoria, mudanças e recursos.	Sim	Saídas devem gerar ações, responsáveis e prazos.	Ata; plano de ação; orçamento; acompanhamento.
10.1	Tratar não conformidades, causas, correções, ações e eficácia.	Sim	RNC-001 a RNC-006 demonstram necessidade de processo robusto.	PO-003; RNC-000; evidências de eficácia.
10.2	Melhorar continuamente adequação, suficiência e eficácia do SGSI.	Sim	Ameaças, tecnologia e requisitos mudam continuamente.	Backlog; lições; análise crítica; melhorias.

Anexo C - Matriz de Aplicabilidade e Diretrizes dos Controles do Anexo A

> Esta matriz funciona como base de trabalho para a Declaração de Aplicabilidade. O status final deve ser validado contra a matriz de riscos, a arquitetura real, os contratos e as evidências.

ID	Controle	Descrição/diretriz 1 IT	Aplicável?	Jus
A.5.1	Políticas de segurança da informação	Manter este Manual e políticas derivadas aprovadas, comunicadas, revisadas e coerentes com riscos e requisitos.	Aplicável	Ne rec esc der gov pro cor a a IT.
A.5.2	Papéis e responsabilidades de segurança	Definir responsabilidades no MA-001, RACI, nomeações e contratos; manter substitutos e alçadas.	Aplicável	Ne rec esc der gov pro cor a a IT.
A.5.3	Segregação de funções	Separar solicitação, aprovação, execução e revisão; aplicar dupla aprovação e logs quando houver acumulação.	Aplicável	Ne rec esc der gov pro cor a a IT.
A.5.4	Responsabilidades da direção	Exigir cumprimento, prover recursos, decidir riscos e apoiar investigação e melhoria.	Aplicável	Ne rec esc der gov pro cor a a IT.
A.5.5	Contato com autoridades	Manter contatos atualizados com ANPD, autoridades policiais,	Aplicável	Ne rec esc

		reguladores e órgãos de trânsito, conforme aplicável.		der gov pro cor a a IT.
A.5.6	Contato com grupos especializados	Acompanhar fontes confiáveis, comunidades técnicas, fornecedores e alertas de segurança.	Aplicável - proporcional/parcial	Ne rec esc der gov pro cor a a IT.
A.5.7	Inteligência de ameaças	Coletar, avaliar e transformar inteligência em riscos, alertas, patches, bloqueios e treinamento.	Aplicável - proporcional/parcial	Ne rec esc der gov pro cor a a IT.
A.5.8	Segurança em projetos	Incluir segurança, privacidade, riscos, continuidade e aceite em projetos e mudanças.	Aplicável	Ne rec esc der gov pro cor a a IT.
A.5.9	Inventário de informações e ativos	Inventariar dados, sistemas, APIs, equipamentos, contas, documentos, fornecedores e proprietários.	Aplicável	Ne rec esc der gov pro cor a a IT.

A.5.10	Uso aceitável de informações e ativos	Aplicar regras de uso aceitável, canais autorizados, proteção e reporte de desvios.	Aplicável	Ne rec esc der gov pro cor a a IT.
A.5.11	Devolução de ativos	Recolher equipamentos, crachás, documentos, chaves, certificados e acessos no encerramento.	Aplicável	Ne rec esc der gov pro cor a a IT.
A.5.12	Classificação da informação	Aplicar níveis Público, Interno, Confidencial e Restrito por proprietário e risco.	Aplicável	Ne rec esc der gov pro cor a a IT.
A.5.13	Rotulagem da informação	Rotular documentos, mensagens, exportações e ativos conforme classificação e contexto.	Aplicável	Ne rec esc der gov pro cor a a IT.
A.5.14	Transferência da informação	Autorizar transferências, usar criptografia, autenticação, integridade, logs e minimização.	Aplicável	Ne rec esc der gov

				pro con a a IT.
A.5.15	Controle de acesso	Definir política de acesso por menor privilégio, necessidade e segregação.	Aplicável	Ne rec esc der gov pro con a a IT.
A.5.16	Gestão de identidades	Controlar ciclo de vida de identidades humanas, técnicas, fornecedores e serviços.	Aplicável	Ne rec esc der gov pro con a a IT.
A.5.17	Proteção das informações de autenticação	Armazenar segredos em cofre; proibir compartilhamento e exposição em código/wiki/e-mail.	Aplicável	Ne rec esc der gov pro con a a IT.
A.5.18	Concessão e revisão de direitos de acesso	Aprovar, revisar, alterar e revogar direitos com evidência e periodicidade por criticidade.	Aplicável	Ne rec esc der gov pro con a a IT.

A.5.19	Segurança nas relações com fornecedores	Classificar fornecedores, avaliar riscos e acompanhar controles durante toda a relação.	Aplicável - responsabilidade compartilhada	Ne rec esc der gov pro cor a a IT.
A.5.20	Segurança em acordos com fornecedores	Inserir cláusulas de segurança, privacidade, incidentes, auditoria, SLA, subcontratação e saída.	Aplicável - responsabilidade compartilhada	Ne rec esc der gov pro cor a a IT.
A.5.21	Segurança na cadeia de suprimentos de TIC	Avaliar dependências, componentes, atualizações, procedência, integridade e riscos da cadeia TIC.	Aplicável - responsabilidade compartilhada	Ne rec esc der gov pro cor a a IT.
A.5.22	Monitoramento e mudanças em serviços de fornecedores	Monitorar SLA, incidentes, mudanças, certificações, vulnerabilidades e eficácia dos fornecedores.	Aplicável - responsabilidade compartilhada	Ne rec esc der gov pro cor a a IT.
A.5.23	Segurança no uso de serviços em nuvem	Definir responsabilidade compartilhada, configuração, dados, IAM, logs, backup, região e reversibilidade na nuvem.	Aplicável - responsabilidade compartilhada	Ne rec esc der gov

				pro cor a a IT.
A.5.24	Preparação para gestão de incidentes	Manter PO-014, equipe/alçadas, contatos, canais, ferramentas, playbooks e exercícios.	Aplicável	Ne rec esc der gov pro cor a a IT.
A.5.25	Avaliação e decisão sobre eventos de segurança	Triar alertas, determinar incidente e severidade, registrar decisão e escalonar.	Aplicável	Ne rec esc der gov pro cor a a IT.
A.5.26	Resposta a incidentes de segurança	Conter, erradicar, recuperar, comunicar, preservar evidências e documentar decisões.	Aplicável	Ne rec esc der gov pro cor a a IT.
A.5.27	Aprendizado com incidentes	Executar RCA, atualizar controles, riscos, treinamento e indicadores.	Aplicável	Ne rec esc der gov pro cor a a IT.

A.5.28	Coleta e preservação de evidências	Preservar evidências com integridade, tempo, origem, hash e cadeia de custódia proporcional.	Aplicável - proporcional/parcial	Ne rec esc der gov pro cor a a IT.
A.5.29	Segurança durante interrupções	Manter controles essenciais e regras de emergência durante crises e contingências.	Aplicável - responsabilidade compartilhada	Ne rec esc der gov pro cor a a IT.
A.5.30	Prontidão de TIC para continuidade	Alinhar TIC à BIA, RTO/RPO, redundância, backup, recuperação e testes do MA-005.	Aplicável - responsabilidade compartilhada	Ne rec esc der gov pro cor a a IT.
A.5.31	Requisitos legais, regulatórios e contratuais	Manter matriz de requisitos e verificar mudanças legais, regulatórias e contratuais.	Aplicável	Ne rec esc der gov pro cor a a IT.
A.5.32	Direitos de propriedade intelectual	Controlar licenças, código, marcas, conteúdo, contratos e uso de software.	Aplicável	Ne rec esc der gov

				pro con a a IT.
A.5.33	Proteção de registros	Proteger registros quanto a integridade, acesso, retenção, recuperação e descarte.	Aplicável	Ne rec esc der gov pro con a a IT.
A.5.34	Privacidade e proteção de dados pessoais	Integrar MA-004, minimização, direitos, AIPD/RIPD, incidentes e contratos.	Aplicável	Ne rec esc der gov pro con a a IT.
A.5.35	Análise crítica independente da segurança	Executar auditoria independente e avaliações técnicas proporcionais ao risco.	Aplicável	Ne rec esc der gov pro con a a IT.
A.5.36	Conformidade com políticas e padrões	Verificar aderência por revisões, auditorias, indicadores, amostras e ações corretivas.	Aplicável	Ne rec esc der gov pro con a a IT.

A.5.37	Procedimentos operacionais documentados	Documentar operações críticas com responsáveis, critérios, registros e exceções.	Aplicável	Ne rec esc der gov pro cor a a IT.
A.6.1	Verificação prévia de pessoas	Aplicar verificação proporcional, legal e documentada a funções e terceiros sensíveis.	Aplicável - proporcional/parcial	Pes ter cau pre inc cor pro pap ace
A.6.2	Termos e condições de contratação	Incluir deveres de segurança, confidencialidade, uso aceitável, propriedade e devolução.	Aplicável	Pes ter cau pre inc cor pro pap ace
A.6.3	Conscientização, educação e treinamento	Executar integração, EAD anual, avaliação e trilhas por função.	Aplicável	Pes ter cau pre inc cor pro pap ace
A.6.4	Processo disciplinar	Manter processo disciplinar proporcional, documentado e integrado a RH/Jurídico.	Aplicável - proporcional/parcial	Pes ter cau pre inc

				co pro pap ace
A.6.5	Responsabilidades após mudança ou término	Revogar acessos e manter deveres pós-vínculo; reavaliar acessos em movimentações.	Aplicável	Pes ter cau pre inc co pro pap ace
A.6.6	Acordos de confidencialidade	Formalizar NDAs e revisar validade, escopo, partes e obrigações.	Aplicável	Pes ter cau pre inc co pro pap ace
A.6.7	Trabalho remoto	Aplicar requisitos de dispositivo, MFA, ambiente, VPN/Zero Trust e reporte.	Aplicável - proporcional/parcial	Pes ter cau pre inc co pro pap ace
A.6.8	Relato de eventos de segurança	Disponibilizar canal simples e proteger quem reporta de boa-fé.	Aplicável	Pes ter cau pre inc co pro pap ace

A.7.1	Perímetros de segurança física	Delimitar áreas administrativas e exigir evidências de perímetros nos provedores.	Aplicável - responsabilidade compartilhada	Ap adr por res cor aos e ir for
A.7.2	Entrada física controlada	Controlar entrada, visitantes, chaves e acessos físicos locais e terceirizados.	Aplicável - responsabilidade compartilhada	Ap adr por res cor aos e ir for
A.7.3	Proteção de escritórios e instalações	Proteger recepção, postos, documentos e salas; evitar exposição ao público.	Aplicável - proporcional/parcial	Ap adr por res cor aos e ir for
A.7.4	Monitoramento de segurança física	Adotar monitoramento proporcional local e exigir controles/certificações dos datacenters.	Aplicável - responsabilidade compartilhada	Ap adr por res cor aos e ir for
A.7.5	Proteção contra ameaças físicas e ambientais	Avaliar incêndio, água, energia, clima, furto e ameaças em locais e provedores.	Aplicável - responsabilidade compartilhada	Ap adr por res cor aos e ir for

A.7.6	Trabalho em áreas seguras	Definir regras para áreas restritas; acompanhar visitantes e limitar dispositivos.	Aplicável - proporcional/parcial	Ap adr por res cor aos e ir for
A.7.7	Mesa limpa e tela limpa	Aplicar bloqueio de tela, guarda de documentos e descarte seguro.	Aplicável	Ap adr por res cor aos e ir for
A.7.8	Localização e proteção de equipamentos	Posicionar e proteger equipamentos contra acesso, dano, observação e furto.	Aplicável - proporcional/parcial	Ap adr por res cor aos e ir for
A.7.9	Segurança de ativos fora das instalações	Controlar notebooks, celulares, mídias e documentos em deslocamento ou trabalho remoto.	Aplicável - proporcional/parcial	Ap adr por res cor aos e ir for
A.7.10	Mídias de armazenamento	Restringir mídias removíveis, criptografar, inventariar e descartar com segurança.	Aplicável - proporcional/parcial	Ap adr por res cor aos e ir for

A.7.11	Serviços de utilidade de apoio	Assegurar energia e conectividade proporcionais localmente e redundância nos provedores.	Aplicável - responsabilidade compartilhada	Ap adr por res cor aos e ir for
A.7.12	Segurança do cabeamento	Proteger cabeamento local; exigir segurança e redundância em instalações terceirizadas.	Aplicável - responsabilidade compartilhada	Ap adr por res cor aos e ir for
A.7.13	Manutenção de equipamentos	Autorizar manutenção, registrar intervenções e proteger dados antes/depois do serviço.	Aplicável - responsabilidade compartilhada	Ap adr por res cor aos e ir for
A.7.14	Descarte ou reutilização segura de equipamentos	Sanitizar, destruir ou comprovar eliminação antes de reutilização ou descarte.	Aplicável - responsabilidade compartilhada	Ap adr por res cor aos e ir for
A.8.1	Dispositivos endpoint do usuário	Aplicar baseline, atualização, EDR, firewall, criptografia, bloqueio e inventário.	Aplicável	Os dep apl ide rec bar des seg

A.8.2	Direitos de acesso privilegiado	Restringir privilégios, usar PAM/cofre, MFA, acesso temporário e revisão frequente.	Aplicável	Os dep apl ide rec bar des seg
A.8.3	Restrição de acesso à informação	Implementar autorização por função, objeto, cliente, dado e ambiente.	Aplicável	Os dep apl ide rec bar des seg
A.8.4	Acesso ao código-fonte	Restringir repositórios, branches, chaves, exportações e revisão de alterações.	Aplicável	Os dep apl ide rec bar des seg
A.8.5	Autenticação segura	Aplicar MFA, protocolos seguros, proteção contra força bruta, sessão e recuperação segura.	Aplicável	Os dep apl ide rec bar des seg
A.8.6	Gestão de capacidade	Monitorar recursos, tendências, limites e capacidade para atender SLA e continuidade.	Aplicável - proporcional/parcial	Os dep apl ide rec bar des seg

A.8.7	Proteção contra malware	Aplicar EDR/antimalware, filtragem, restrições, atualização e resposta.	Aplicável	Os dep apl ide rec bar des seg
A.8.8	Gestão de vulnerabilidades técnicas	Manter inventário, fontes, varredura, classificação, SLA, exceção e validação.	Aplicável	Os dep apl ide rec bar des seg
A.8.9	Gestão de configuração	Manter baselines, infraestrutura como código quando possível, revisão e detecção de desvio.	Aplicável	Os dep apl ide rec bar des seg
A.8.10	Exclusão de informação	Eliminar dados de forma autorizada, verificável e coerente com retenção e backups.	Aplicável	Os dep apl ide rec bar des seg
A.8.11	Mascaramento de dados	Usar mascaramento, anonimização ou dados sintéticos em testes e exibições.	Aplicável - proporcional/parcial	Os dep apl ide rec bar des seg

A.8.12	Prevenção de vazamento de dados	Aplicar minimização, restrição de canais, alertas e DLP proporcional ao risco.	Aplicável - proporcional/parcial	Os dep apl ide rec bar des seg
A.8.13	Backup de informação	Executar backups protegidos, segregados e testados conforme RPO/RTO.	Aplicável	Os dep apl ide rec bar des seg
A.8.14	Redundância de recursos de processamento	Implementar redundância e failover em recursos críticos por arquitetura e contratos.	Aplicável - responsabilidade compartilhada	Os dep apl ide rec bar des seg
A.8.15	Registro de eventos - logs	Gerar, proteger, reter e revisar logs de eventos relevantes.	Aplicável	Os dep apl ide rec bar des seg
A.8.16	Atividades de monitoramento	Monitorar sistemas, redes, APIs, identidades e comportamento; tratar alertas.	Aplicável	Os dep apl ide rec bar des seg

A.8.17	Sincronização de relógios	Sincronizar relógios com fontes confiáveis e monitorar desvios.	Aplicável	Os dep apl ide rec bar des seg
A.8.18	Uso de programas utilitários privilegiados	Restringir utilitários capazes de contornar controles e registrar seu uso.	Aplicável	Os dep apl ide rec bar des seg
A.8.19	Instalação de software em sistemas operacionais	Permitir instalação somente por processo autorizado, fonte confiável e registro.	Aplicável	Os dep apl ide rec bar des seg
A.8.20	Segurança de redes	Documentar topologia, firewall, acesso remoto, criptografia e monitoramento de rede.	Aplicável - responsabilidade compartilhada	Os dep apl ide rec bar des seg
A.8.21	Segurança dos serviços de rede	Definir requisitos, SLA e segurança para internet, VPN, DNS, e-mail, cloud e links.	Aplicável - responsabilidade compartilhada	Os dep apl ide rec bar des seg

A.8.22	Segregação de redes	Separar usuários, administração, desenvolvimento, teste, produção e serviços sensíveis.	Aplicável	Os dep apl ide rec bar des seg
A.8.23	Filtragem de conteúdo web	Filtrar conteúdo malicioso e categorias de risco; controlar exceções e privacidade.	Aplicável - proporcional/parcial	Os dep apl ide rec bar des seg
A.8.24	Uso de criptografia	Definir padrões criptográficos, ciclo de chaves, certificados e exceções.	Aplicável	Os dep apl ide rec bar des seg
A.8.25	Ciclo de vida de desenvolvimento seguro	Integrar segurança ao planejamento, design, construção, teste, implantação e retirada.	Aplicável	Os dep apl ide rec bar des seg
A.8.26	Requisitos de segurança de aplicações	Documentar requisitos de segurança e privacidade antes do desenvolvimento/aquisição.	Aplicável	Os dep apl ide rec bar des seg

A.8.27	Arquitetura e engenharia segura	Aplicar princípios de arquitetura segura, defesa em profundidade e redução de superfície.	Aplicável	Os dep apl ide rec bar des seg
A.8.28	Codificação segura	Adotar padrões de codificação, revisão, linting, tratamento de erros e proteção de segredos.	Aplicável	Os dep apl ide rec bar des seg
A.8.29	Testes de segurança no desenvolvimento e aceitação	Executar testes de segurança proporcionais antes da aceitação e após mudanças relevantes.	Aplicável	Os dep apl ide rec bar des seg
A.8.30	Desenvolvimento terceirizado	Controlar requisitos, acesso, código, testes, propriedade e evidências de terceiros.	Aplicável - proporcional/parcial	Os dep apl ide rec bar des seg
A.8.31	Separação de ambientes de desenvolvimento, teste e produção	Segregar ambientes, credenciais, dados e pipelines; restringir promoção a produção.	Aplicável	Os dep apl ide rec bar des seg

A.8.32	Gestão de mudanças	Aplicar PO-007 e atender ao RNC-004 em todas as mudanças relevantes.	Aplicável	Os dep apl ide rec bar des seg
A.8.33	Informações de teste	Usar dados sintéticos/mascarados, autorizar cópias e eliminar após finalidade.	Aplicável	Os dep apl ide rec bar des seg
A.8.34	Proteção de sistemas durante testes de auditoria	Planejar testes de auditoria para evitar indisponibilidade, alteração ou exposição.	Aplicável - proporcional/parcial	Os dep apl ide rec bar des seg

Anexo D - Matriz de Evidências Mínimas para Auditoria

Domínio	Evidência documental	Evidência operacional/técnica	Teste de eficácia
Governança	Política, escopo, RACI, atas, objetivos.	Decisões, orçamento, comunicações e acompanhamento.	Entrevista com Direção e rastreamento de ações.
Riscos	Metodologia, matriz, PTR e SoA.	Tickets, controles e aprovações.	Amostra de risco alto até evidência e risco residual.

Acessos	PO-016, perfis, aprovações e revisões.	Export de usuários, MFA, PAM e logs.	Amostra de admissão, movimentação e desligamento.
Fornecedores	Matriz, due diligence, contratos e SLAs.	Relatórios, reuniões, incidentes e acessos.	Amostra de fornecedor crítico e reversibilidade.
Mudanças	PO-007, modelos e critérios.	Tickets, pipelines, testes e rollback.	Amostra de mudança recente em produção.
Vulnerabilidades	PO-019, escopo, SLA e exceções.	Scanner, tickets, patches e retestes.	Selecionar achado e comprovar correção.
Hardening	Baselines e padrões.	Configurações, IaC, desvios e revisões.	Conferência técnica de amostra.
Logs	Política, fontes, retenção e alçadas.	SIEM/logs, alertas, integridade e tempo.	Simular evento e verificar detecção/rastreabilidade.
Backup/Continuidade	PO-006, MA-005, BIA, RTO/RPO.	Jobs, cópias, falhas, restaurações e failover.	Teste de restauração e exercício de mesa.
Incidentes	PO-014/015, playbooks e contatos.	Tickets, linha do tempo, evidências e RCA.	Exercício ou amostra de evento real/simulado.
Treinamento	Plano, conteúdo, público e termos.	Logs EAD, notas, pendências e reciclagem.	Entrevistas e simulação de phishing/reporte.
Desenvolvimento	SDLC, requisitos, padrões e aceite.	Repositório, revisão, SAST/DAST/SCA e pipelines.	Amostra de release até requisitos e testes.
Privacidade	MA-004, ROPA, mapa e AIPD/RIPD.	Contratos, atendimentos, incidentes e retenção.	Amostra de fluxo de dado ponta a ponta.

Outline Wiki	Regras, lista mestra, classificação e acesso.	Usuários, grupos, compartilhamentos, logs e backup.	Amostra de documento, versão, permissão e restauração.