INVISIBLE CORE

| O Mínimo Defensável |

CIS Control
NIST CSF
ISO/IEC 27001
PCI DSS
LGPD/GDPR

HS IC

e-Books

Série: High Security
Invisible Core - HSIC

EDITORA JP

JOÃO ROBERTO PERES

JOÃO ROBERTO PERES

INVISIBLE CORE

— O Mínimo Defensável —

São Paulo

Editora JP

Dados Internacionais de catalogação na publicação (CIP) de acordo com o ISBD.

P512i Peres, João Roberto,

Invisible Core – O mínimo defensável.

João Roberto Peres, – 1ª Ed. – São Paulo: Edição 2026.

Recurso Digital – Formato PDF 5500 Kb - Requisitos do Sistema: Adobe AcrobatReader ou similar. Modo de acesso w.w.w..

123 p.: 21 x 29,7 cm.
Inclui Bibliografia e anexos
ISBN 978-65-01-90427-6 (Recurso Digital) Registro CBL Câmara Brasileira do Livro.

1. Segurança da informação 2. Proteção de dados 3. Governança corporativa 4. Gestão de riscos 5. CIS Controls 6. Compliance 7. LGPD - Lei Geral de Proteção de Dados I. Título. II. Série.

CDD 658.478 (Gestão de riscos e segurança da informação).

CDU 004.056:658 (Segurança da informação aplicada à gestão empresarial).

Consulta registro ISBN CBL: https://www.cblservicos.org.br/isbn/pesquisa/

1º volume da série: High Security Invisible Core “HSIC”.

Hash SHA512 do texto original antes da geração .PDF – arquivo em .docx sem Hash.

Declaração

Este trabalho foi propositalmente desenvolvido utilizando metodologia de escrita assistida por IA, onde 12 sistemas de linguagem de grande escala (LLMs) geraram conteúdo substancial de base sob direção estratégica do autor. O processo seguiu protocolo rigoroso MDM-AI: (1) planejamento estrutural humano detalhado, (2) geração de seções via prompts especificados, (3) pesquisas e revisões críticas multicamadas, (4) verificação de originalidade e plágio estatístico, (5) transformação autoral para garantir voz distintiva, entre outros. Este documento indica metodologia de apoio humano-algorítmica transparente, mas não representa delegação de autoria, sendo o autor humano único responsável pelo conteúdo. Embora tenham sido adotados todos os cuidados metodológicos de escrita acadêmica, incluindo verificação por ferramentas antiplágio e uso responsável de IA, não se descarta a possibilidade de coincidências textuais involuntárias com obras existentes, dadas a vastidão da literatura sobre segurança cibernética e tecnologias emergentes. Tais eventuais sobreposições, se detectadas, não configuram plágio intencional.

Sumário

PREFÁCIO

PREFÁCIO DO AUTOR (Leitura fundamental para compreender a obra)

O Paradoxo do Óbvio

Existe um fenômeno curioso que observo há mais de quatro décadas atuando como Consultor em segurança corporativa. Chamo-o de paradoxo do óbvio: quanto mais evidente é uma vulnerabilidade, menos urgência ela desperta. Quanto mais básica a solução, menor a probabilidade de ser implementada.

Converso regularmente com executivos, conselheiros, empresários e gestores de tecnologia. A maioria deles concorda, sem hesitação, que segurança da informação é importante. Alguns até mencionam casos de empresas que sofreram ataques devastadores. Quase todos conseguem citar ao menos uma manchete sobre ransomware, vazamento de dados ou fraudes digitais. E, no entanto, quando pergunto sobre o inventário de ativos de suas próprias organizações, sobre a política de senhas, sobre os backups, sobre quem tem acesso administrativo aos sistemas críticos, as respostas oscilam entre o vago e o constrangido.

Não é que essas pessoas sejam negligentes ou ignorantes. Muitas delas administram negócios complexos, tomam decisões financeiras sofisticadas, navegam ambientes regulatórios intrincados. O problema é outro: segurança da informação, especialmente a segurança básica, sofre de um déficit crônico de urgência. Parece sempre haver algo mais importante para fazer, mais urgente para resolver, mais estratégico para discutir. O básico pode esperar. Até que não pode mais.

A Ilusão da Imunidade

Em muitas décadas trabalhando com segurança, desenvolvi uma habilidade involuntária: consigo identificar, nos primeiros minutos de uma reunião, qual será a objeção principal. As variações são muitas, mas o tema subjacente é sempre o mesmo.

"Nunca tivemos problemas." Esta é a mais comum. Organizações que operam há anos sem incidentes visíveis desenvolvem uma espécie de imunidade percebida. O raciocínio implícito é estatístico: se nada aconteceu até agora, provavelmente nada acontecerá. O que esse raciocínio ignora é que muitos incidentes permanecem não detectados por meses ou anos. Dados do relatório "Cost of a Data Breach 2025"[1] da IBM indicam que o tempo médio para identificar e conter uma violação é de 241 dias, embora violações que ultrapassam 200 dias resultem em custos significativamente maiores. A ausência de problemas conhecidos não significa ausência de problemas.

[1] Relatório IBM 2025 – Disponível em: https://www.ibm.com/reports/data-breach - Acesso jan. 2026.

"Já investimos em segurança." Esta objeção geralmente vem acompanhada de uma lista: firewall, antivírus, backup em nuvem, talvez um appliance de segurança adquirido há alguns anos e diversas Políticas e Procedimentos. O problema é que segurança não funciona como um produto que se compra uma vez e está resolvido. Funciona como um processo contínuo que exige configuração adequada, atualização constante, monitoramento e, principalmente, integração com as operações do negócio. Um firewall mal configurado oferece falsa sensação de segurança. Um antivírus desatualizado é pouco mais que decoração digital. Um backup que nunca foi testado pode não funcionar quando for necessário. Uma documentação que ninguém conhece e procedimentos que não são reais, levam ao desastre.

"Somos pequenos demais para ser alvo." Esta é particularmente perigosa. Pequenas e médias empresas frequentemente acreditam que atacantes focam apenas em grandes corporações, bancos, governos. A realidade é precisamente oposta. Ataques automatizados não discriminam por porte. Ransomware não verifica o faturamento da vítima antes de criptografar seus arquivos. Na verdade, organizações menores frequentemente são alvos preferenciais justamente porque investem menos em proteção. Dados da Accenture indicam que 43% dos ataques cibernéticos visam pequenas empresas, mas apenas 14% delas estão preparadas para se defender.

"Segurança é custo." Esta objeção revela uma compreensão equivocada da natureza do risco. Segurança da informação não é despesa operacional comparável a aluguel ou energia elétrica. É gestão de risco comparável a investimento em seguro, prevenção de incêndio ou atendimento a compliance regulatório. O custo de não investir em segurança básica só se torna visível quando o incidente acontece, e nesse momento os valores envolvidos frequentemente superam muito em ordens de magnitude o que teria sido necessário para prevenção. Uma empresa que economiza alguns milhares de reais evitando controles básicos pode enfrentar custos de centenas de milhares, ou milhões, em resposta a incidentes, multas regulatórias, perda de clientes e danos reputacionais.

O Mínimo que Não é Feito

Aqui chegamos ao cerne do problema que motivou este livro. Não estou falando de segurança sofisticada. Não estou propondo investimentos milionários em centros de operações de segurança, equipes dedicadas de "threat hunting", ou tecnologias de ponta baseadas em inteligência artificial. Estou falando do básico. Do mínimo. Do que deveria ser óbvio.

Saber quais computadores e dispositivos existem na rede. Saber quais softwares estão instalados. Garantir que senhas não sejam triviais. Restringir acessos administrativos a quem realmente precisa deles. Fazer backup e testar se funciona. Atualizar sistemas quando correções de segurança são publicadas. Treinar pessoas para reconhecer tentativas de fraude.

Nenhuma dessas medidas é revolucionária. Nenhuma exige orçamentos extraordinários. Nenhuma demanda especialista com décadas de experiência. E, no entanto, a maioria das organizações que sofrem incidentes graves falhou em uma ou mais dessas medidas básicas. Os relatórios anuais Verizon Data Breach Investigations Report (DBIR)[2], bem como estudos de outros fornecedores, vêm mostrando de forma consistente que credenciais roubadas, vulnerabilidades exploradas, configurações incorretas e o fator humano respondem pela maior parte dos vetores iniciais de ataque observados em violações reais.

O problema, portanto, não é falta de conhecimento sobre o que fazer. O problema é a lacuna entre saber e fazer. Entre reconhecer a importância e efetivamente implementar. Entre concordar com o diagnóstico e tomar a medicação.

Por Que Este Livro Existe

Este livro nasceu de uma frustração e de uma descoberta.

A frustração vem de anos observando o mesmo padrão se repetir. Organizações que poderiam ter evitado incidentes com medidas simples. Executivos que descobrem tarde demais que o básico não estava sendo feito. Empresas que investem em soluções sofisticadas enquanto negligenciam fundamentos. A sensação de que existe um descompasso fundamental entre o que a comunidade de segurança sabe ser necessário e o que efetivamente acontece nas organizações.

A solução prática já não é nova, há muitos anos ministro cursos sobre as práticas do “CIS Critical Security Controls” para grupos de profissionais de diferentes setores. O CIS Controls é um framework objetivo desenvolvido pelo Center for Internet Security, uma organização sem fins lucrativos, que consolida quase duas décadas de experiência da comunidade internacional de segurança em uma lista priorizada de ações defensivas. O framework é gratuito, acessível, muito bem documentado e foi desenhado especificamente para ser implementável por organizações de qualquer porte.

O que me surpreende durante esses cursos que ministro de CIS Control não é a sofisticação dos participantes. Todos são profissionais competentes, alguns com anos de experiência em tecnologia. O que me surpreende é a descoberta de perceber que mesmo esse público, relativamente informado, desconhecia aspectos fundamentais do framework. Não sabiam, por exemplo, que o CIS Controls define três níveis de implementação (chamados Implementation Groups), e que o primeiro nível (IG1) contém apenas 56 salvaguardas consideradas essenciais para qualquer organização, independentemente de porte ou setor. Não sabiam que estudos do próprio CIS demonstram que a implementação desse primeiro nível defende contra

[2] VERIZON. 2025 Data Breach Investigations Report. 2025. Disponível em: https://www.verizon.com/business/resources/reports/dbir/. Acesso em: jan. 2026.

74% das técnicas de ataque documentadas no MITRE ATT&CK, que é a matriz de referência utilizada globalmente para catalogar táticas de adversários (atacantes hackers).

Se profissionais de tecnologia desconheciam esses elementos, o que dizer de executivos, conselheiros, advogados, empresários? Como esperar que tomem decisões informadas sobre a simplicidade da segurança se o conhecimento que fundamentaria essas decisões permanece encapsulado em percepção sobre documentos técnicos complexos, conferências especializadas e comunidades de praticantes avançada?

O Propósito desta Obra

Este livro é uma tradução. Não no sentido linguístico, embora o CIS Controls seja originalmente publicado em inglês. É uma tradução de registro: do técnico para o estratégico, do operacional para o decisório, do jargão de especialistas para a linguagem de quem precisa decidir sem ser especialista.

Meu objetivo não é formar profissionais de segurança. Para isso existem certificações, cursos técnicos, laboratórios práticos. Meu objetivo é capacitar pessoas que tomam decisões (executivos, conselheiros, gestores, empresários, advogados) a compreender o que o CIS Controls representa, por que é relevante para suas organizações, e como utilizá-lo como instrumento de governança e gestão de risco.

O título escolhido, “InvisibleCore | O Mínimo Defensável”, captura a essência do que proponho. "Invisible" porque segurança bem feita é, paradoxalmente, invisível: funciona em segundo plano, não atrapalha operações, não demanda atenção constante. "Core" porque estamos tratando do núcleo, do essencial, do que não pode ser negligenciado. "Mínimo Defensável" porque o objetivo não é perfeição (inatingível e insustentável), mas sim um patamar de proteção que seja, simultaneamente, alcançável por qualquer organização e suficiente para demonstrar diligência razoável.

Esse último ponto merece ênfase. Vivemos em um ambiente regulatório onde a LGPD exige "medidas técnicas e administrativas aptas a proteger os dados pessoais", onde o Código Civil estabelece responsabilidade por danos causados por negligência, onde contratos comerciais frequentemente incluem cláusulas de segurança da informação, onde seguradoras condicionam cobertura à demonstração de controles básicos. Nesse contexto, a ausência de medidas mínimas de segurança não é apenas um risco técnico. É um risco jurídico, contratual, reputacional.

O CIS Controls oferece uma resposta a esse desafio. Uma organização que implementa o IG1 (com as 56 salvaguardas essenciais) e documenta essa implementação possui evidência concreta de que adotou o cuidado que dela se esperava. Não é garantia de imunidade a incidentes, nenhum framework oferece isso. Mas é demonstração de diligência que pode fazer diferença significativa em uma

fiscalização regulatória, em um litígio por vazamento de dados, ou em uma negociação com seguradoras.

Leitura Imprescindível

Antes de prosseguir com este livro, recomendo enfaticamente que o leitor acesse e examine dois documentos disponíveis gratuitamente no site do Center for Internet Security (https://www.cisecurity.org/controls/v8-1):

CIS Critical Security Controls é o documento principal do framework. Contém a descrição completa dos 18[3] controles e suas 153 salvaguardas da Versão 8.1, incluindo orientações sobre procedimentos, ferramentas e classificação por Implementation Group. Mesmo que o leitor não tenha interesse em detalhes técnicos, a leitura da introdução e das seções "Why is this Control critical?" de cada controle oferece uma visão panorâmica do raciocínio por trás do framework.

Guide to Implementation Groups (IG) é o documento que explica como as organizações devem escolher seu nível de implementação com base em fatores como porte, complexidade, tipos de dados tratados, recursos disponíveis e perfil de ameaças. Este guia é particularmente relevante para executivos e gestores porque traduz conceitos técnicos em critérios de decisão gerencial.

Esses documentos são a fonte primária. Este livro é complemento, não substituto. Meu papel é contextualizar, explicar, conectar com a realidade brasileira e com as preocupações específicas de quem toma decisões sem ser especialista em segurança. Mas a autoridade final sobre o que o CIS Controls prescreve está nos documentos oficiais do CIS.

O Que o Leitor Encontrará

Este livro está organizado em quatro partes.

A Parte I apresenta o CIS Controls para quem não o conhece, explicando o que é, o que não é, como se relaciona com outros frameworks, e por que se tornou referência internacional de diligência em segurança.

A Parte II examina o CIS Controls como instrumento de decisão, explorando sua relação com responsabilidade legal, com a LGPD, com seguros cibernéticos, e com a priorização de investimentos em contextos de recursos limitados.

A Parte III conecta o CIS Controls com os outros volumes da série High Security Invisible Core (HSIC), demonstrando como o framework fundamenta conceitos de

[3] CIS Control 18 controles. Disponível em: https://www.cisecurity.org/controls/cis-controls-list - acesso jan. 2026.

Imunidade Digital, governança de identidades não humanas e preparação para ameaças quânticas.

A Parte IV oferece orientações práticas por perfil de leitor (executivos, gestores de TIC, advogados, PMEs), além de discutir os limites do framework e como complementá-lo quando necessário.

Os apêndices incluem roteiros de perguntas essenciais para avaliação de postura por perfil de leitor, correlação entre os controles CIS IG1, LGPD e requisitos de seguradoras, e glossário executivo com termos traduzidos para linguagem de negócio.

Um Convite

Encerro este prefácio com um convite e uma advertência.

O convite é para que o leitor aborde este livro com disposição para questionar suas próprias suposições. Se você acredita que sua organização está adequadamente protegida, pergunte-se: em que evidência essa crença se baseia? Se você acredita que segurança é problema exclusivo da área de TI, pergunte-se: quem responde juridicamente quando um incidente acontece? Se você acredita que controles básicos já estão implementados, pergunte-se: quando foi a última vez que alguém verificou?

A advertência é que conhecimento gera responsabilidade. Após ler este livro, você não poderá alegar desconhecimento sobre o que constitui o mínimo defensável em segurança da informação. A decisão de implementar ou não implementar será consciente, e as consequências dessa decisão serão suas.

O CIS Controls não é panaceia. Não resolve todos os problemas de segurança, não elimina todos os riscos, não substitui julgamento humano e adaptação ao contexto específico de cada organização. Mas oferece algo valioso: um ponto de partida concreto, validado pela experiência, escalável conforme recursos disponíveis, e reconhecido como referência de diligência razoável.

O básico parece óbvio até que você percebe que não está sendo feito. E quando essa percepção chega, frequentemente, é tarde demais.

A hora de começar é agora.

São Paulo, janeiro de 2026

João Roberto Peres

PARTE I: O CIS Control a base da base

CAPÍTULO 1 – Segurança, Problema ou Solução

A Confusão que Paralisa

Existe um padrão recorrente nas organizações brasileiras quando o tema segurança da informação surge nas reuniões de diretoria. Alguém menciona "framework", outro fala em "certificação", um terceiro pergunta sobre "compliance", e a conversa rapidamente se dissolve em um emaranhado de siglas que ninguém domina completamente. ISO 27001, NIST, SOC 2, PCI DSS, CIS Controls. A impressão é de que segurança cibernética exige um diploma em sopa de letrinhas para ser compreendida.

Essa confusão não é acidental. O mercado de segurança da informação cresceu nas últimas duas décadas alimentando-se da complexidade. Consultorias vendem projetos de implementação de frameworks como se fossem empreitadas de engenharia civil. Fabricantes de software prometem conformidade automática com dezenas de regulamentações mediante a compra de suas soluções. Certificadoras oferecem selos que supostamente atestam maturidade em segurança. No meio dessa cacofonia comercial, executivos e gestores acabam paralisados, incapazes de distinguir o essencial do acessório, o obrigatório do opcional, o útil do meramente vendável.

A pergunta que deveria orientar qualquer discussão sobre segurança é simples: segurança da informação é um problema a ser resolvido ou uma solução a ser construída? A resposta determina a postura de toda a organização. Quem enxerga segurança como problema busca eliminá-la, ou terceiriza, delega, compra produtos que prometem fazer o incômodo desaparecer. Quem a compreende como solução reconhece que proteger ativos digitais é parte indissociável da operação, tão estruturante quanto a gestão financeira ou a logística.

O CIS Controls surge nesse cenário como instrumento gratuito para quem escolheu a segunda postura. Não é norma legal. Não é certificação. Não é produto. É, na sua essência, uma lista priorizada de ações defensivas que a comunidade internacional de segurança considera fundamentais para proteger organizações contra os ataques mais comuns e destrutivos. Desenvolvido pelo Center for Internet Security com base em dados reais de incidentes, o framework traduz a pergunta abstrata: "como me proteger?", em respostas concretas e sequenciadas. Nada mais, nada menos.

Origem: Da Trincheira para o Papel

O CIS Controls não nasceu em um comitê de padronização nem em um departamento de marketing de empresa de tecnologia. Sua origem está nas

trincheiras da defesa cibernética, especificamente na experiência acumulada por profissionais que responderam a incidentes reais em organizações reais.

No início dos anos 2000, a comunidade de segurança enfrentava um problema prático, havia conhecimento abundante sobre como atacantes operavam, mas esse conhecimento estava disperso em relatórios técnicos, conferências especializadas e na memória de profissionais experientes. Não existia uma consolidação acessível que dissesse, de forma clara e priorizada, o que uma organização deveria fazer primeiro para se proteger.

A resposta inicial veio do SANS Institute, uma organização de pesquisa e treinamento em segurança, que em 2008 publicou o que ficou conhecido como SANS Top 20[4]. A lista foi construída a partir de uma pergunta simples: considerando os ataques que realmente acontecem, quais controles defensivos teriam impedido ou mitigado a maior parte deles? A resposta não veio de teoria acadêmica, mas da análise forense de incidentes, da experiência de equipes de resposta, e do conhecimento prático de quem enfrentava invasores diariamente.

Em 2015, a gestão dessa lista foi transferida para o Center for Internet Security (CIS), uma organização sem fins lucrativos dedicada a desenvolver e disseminar melhores práticas de segurança. Sob a administração do CIS, o framework passou por revisões sucessivas, incorporando novas ameaças e adaptando-se a mudanças tecnológicas como computação em nuvem e trabalho remoto. A versão atual, 8.1, publicada em junho de 2024, representa quase duas décadas de refinamento contínuo.

O que diferencia o CIS Controls de outros frameworks é justamente essa origem pragmática. Cada controle existe porque a experiência demonstrou que sua ausência facilita ataques específicos. Não há controle no CIS que esteja lá por razões teóricas ou porque "parece uma boa ideia". Todos foram validados contra dados reais de incidentes.

O que o CIS Controls Não É

Para compreender o CIS Controls, é útil começar pelo que ele não é. Essa delimitação negativa ajuda a evitar expectativas desalinhadas e frustrações posteriores.

Não é norma legal. Nenhuma lei brasileira ou internacional obriga organizações a implementar o CIS Controls. Diferentemente da LGPD (Lei Geral de Proteção de Dados), que estabelece obrigações legais com penalidades previstas, ou de regulamentações setoriais como as do Banco Central para instituições financeiras, o CIS Controls não tem força de lei. Sua adoção é voluntária.

[4] CENTER FOR INTERNET SECURITY. The CIS Critical Security Controls for Effective Cyber Defense. 2015. Disponível em: https://en.wikipedia.org/wiki/The_CIS_Critical_Security_Controls_for_Effective_Cyber_Defense - Acesso jan. 2026.

Não é certificação. Não existe um selo "CIS Controls Certified" oficial, que organizações possam ostentar em seus materiais de marketing. Diferentemente da ISO 27001, que possui um processo formal de auditoria e certificação por organismos acreditados, o CIS Controls não oferece certificação institucional. Existem ferramentas de autoavaliação, como o CIS CSAT (Controls Self Assessment Tool), mas estas servem para diagnóstico interno, não para atestação externa.

Não é produto comercial. O CIS Controls está disponível gratuitamente no site do Center for Internet Security. Não há licença a ser adquirida, não há assinatura a ser renovada, não há versão "enterprise" com funcionalidades adicionais. O documento completo, incluindo todas as salvaguardas e orientações de implementação, pode ser baixado por qualquer pessoa sem custo.

Não é um guia de implementação técnica. O CIS Controls descreve o que deve ser feito, não como fazer. Para orientações técnicas detalhadas sobre configuração de sistemas, o CIS oferece os CIS Benchmarks, que são documentos separados com configurações específicas para cada plataforma tecnológica. Os Controls estabelecem objetivos; os Benchmarks detalham implementações.

Não é um substituto para outros frameworks. O CIS Controls coexiste com, e complementa, outros frameworks de segurança. Uma organização pode (e frequentemente deve) utilizar o CIS Controls junto com ISO 27001, NIST Cybersecurity Framework, COBIT, ou qualquer outro modelo de governança de segurança. O CIS inclusive publica mapeamentos oficiais entre seus controles e outros frameworks, facilitando a integração.

O que o CIS Controls é

Feitas as delimitações negativas, podemos afirmar positivamente o que o CIS Controls representa.

É uma lista priorizada de ações defensivas. O framework consiste em 18 controles de alto nível, subdivididos em 153 salvaguardas (safeguards) específicas. Cada salvaguarda representa uma ação concreta que uma organização pode implementar para melhorar sua postura de segurança. A priorização é explícita: os controles são ordenados de forma que os primeiros tenham maior impacto na redução de risco.

É um consenso da comunidade de segurança. O CIS Controls é desenvolvido e mantido por um grupo de voluntários que inclui profissionais de segurança de empresas privadas, órgãos governamentais, instituições acadêmicas e consultorias especializadas. Esse modelo colaborativo garante que o framework reflita experiência diversificada e não os interesses comerciais de um único fabricante.

É uma referência de diligência razoável. Embora não seja norma legal, o CIS Controls é amplamente reconhecido como representação do que constitui cuidado básico em segurança da informação. Auditores, seguradoras e reguladores frequentemente utilizam o CIS Controls como referência para avaliar se uma

organização adotou medidas adequadas de proteção. Em contextos de litígio ou fiscalização, a implementação documentada dos controles pode servir como evidência de diligência.

É um framework escalável. O CIS Controls incorpora o conceito de Implementation Groups (Grupos de Implementação), que permitem às organizações priorizar salvaguardas conforme seu porte, recursos e perfil de risco. Uma pequena empresa pode focar inicialmente no IG1 (Implementation Group 1), que contém 56 salvaguardas consideradas essenciais para qualquer organização. Empresas maiores ou com maior exposição a riscos podem avançar para IG2 e IG3, que adicionam salvaguardas progressivamente mais sofisticadas.

É um ponto de partida, não um destino final. O CIS Controls não pretende cobrir todos os aspectos da segurança da informação. Ele foca nas defesas fundamentais que bloqueiam a maioria dos ataques comuns. Organizações com requisitos específicos de conformidade, setores altamente regulados ou perfis de ameaça diferenciados precisarão complementar o CIS Controls com medidas adicionais apropriadas ao seu contexto.

A Distinção Crítica: Três Situações Juridicamente Distintas

Para executivos e advogados, há uma distinção conceitual no âmbito do CIS Controls que merece atenção especial. Trata-se da diferença entre três situações que, embora possam parecer similares à primeira vista, carregam implicações jurídicas radicalmente distintas.

Primeira situação: não saber que controles e salvaguardas existem. Uma organização que genuinamente desconhece a existência de frameworks de segurança como o CIS Controls pode, em tese, alegar ignorância. Essa alegação, contudo, tornou-se progressivamente mais difícil de sustentar. O CIS Controls é mencionado em documentos regulatórios, recomendações de órgãos de fiscalização, exigências de seguradoras e requisitos contratuais de grandes clientes. A ignorância que poderia ser crível há uma década hoje soa como negligência.

Segunda situação: saber que controles existem e não implementar. Esta é a situação mais perigosa do ponto de vista jurídico. Uma organização que conhece o CIS Controls (ou frameworks equivalentes), compreende sua relevância, mas decide não implementá-los assume um risco consciente. Em caso de incidente, a pergunta inevitável será: por que a organização não adotou medidas que sabia serem necessárias? A resposta "faltou orçamento" raramente convence reguladores ou tribunais, especialmente quando o IG1 do CIS Controls foi explicitamente desenhado para ser implementável com recursos limitados.

Terceira situação: implementar e não documentar. Organizações que implementam controles de segurança mas não documentam adequadamente suas ações enfrentam um problema de prova. Em uma fiscalização da ANPD (Autoridade Nacional de Proteção de Dados) ou em um litígio por vazamento de dados, não basta ter feito; é preciso demonstrar que foi feito. A documentação transforma boas práticas

em evidência defensável. Sem ela, a organização que investiu em segurança pode encontrar-se na mesma posição de quem não investiu.

Essa distinção tripartite tem relevância direta para o tema central deste livro. O CIS Controls, quando adequadamente implementado e documentado, funciona como demonstração objetiva de que a organização adotou o cuidado que dela se esperava. Não elimina riscos nem garante imunidade a incidentes, mas estabelece uma linha de defesa contra alegações de negligência.

Relação com Outros Frameworks

O ecossistema de frameworks de segurança pode parecer um território de competição, onde cada modelo tenta se estabelecer como o padrão definitivo. Na prática, a relação entre frameworks é mais de complementaridade do que de concorrência.

NIST Cybersecurity Framework (CSF). Desenvolvido pelo National Institute of Standards and Technology dos Estados Unidos, o NIST CSF é um framework de referência para gestão de riscos de segurança cibernética. Sua estrutura organiza capacidades de segurança em cinco funções: Identificar, Proteger, Detectar, Responder e Recuperar. O CIS Controls mapeia diretamente para essas funções, com cada salvaguarda classificada conforme a função NIST que ela suporta. A versão 8.1 do CIS Controls, inclusive, incorporou a função "Govern" (Governar) adicionada pelo NIST CSF 2.0, demonstrando o alinhamento entre os frameworks em 2026.

ISO/IEC 27001. A norma internacional para sistemas de gestão de segurança da informação estabelece requisitos para implementar, manter e melhorar continuamente um SGSI (Sistema de Gestão de Segurança da Informação). Enquanto a ISO 27001 é prescritiva sobre processos de gestão, ela é menos específica sobre controles técnicos. O CIS Controls preenche essa lacuna, oferecendo ações concretas que podem ser utilizadas para atender aos controles do Anexo A da ISO 27001.

COBIT. O framework da ISACA para governança e gestão de TI corporativa opera em um nível de abstração superior ao CIS Controls. Enquanto o COBIT trata de processos de governança e alinhamento entre TI e objetivos de negócio, o CIS Controls foca especificamente em defesas contra ameaças cibernéticas. Uma organização pode utilizar COBIT para governança de TI e CIS Controls para operacionalizar a segurança cibernética dentro dessa estrutura de governança.

MITRE ATT&CK. A matriz de táticas, técnicas e procedimentos de adversários mantida pela MITRE Corporation descreve como atacantes operam. O CIS Controls, por sua vez, descreve como defensores devem operar. Os dois frameworks são complementares: o ATT&CK mapeia o comportamento de ameaças, o CIS Controls mapeia as defesas correspondentes. O CIS publica análises que correlacionam implementação dos controles com cobertura contra técnicas do ATT&CK, permitindo que organizações avaliem sua exposição a táticas específicas de adversários.

A mensagem central é que o CIS Controls não compete com esses frameworks; ele coexiste com todos eles, servindo como uma camada operacional de defesas que pode ser integrada a qualquer modelo de governança de segurança que a organização adote.

Por Que Auditores, Seguradoras e Reguladores Adotam o CIS

Uma pergunta legítima que executivos fazem é: se o CIS Controls não é obrigatório, por que tantas entidades o utilizam como referência?

A resposta está na credibilidade que o framework conquistou ao longo de quase duas décadas. Auditores adotam o CIS Controls porque ele oferece uma lista verificável de controles que pode ser auditada de forma objetiva. Cada salvaguarda é suficientemente específica para permitir avaliação de conformidade: ou a organização tem inventário de ativos ou não tem; ou utiliza autenticação multifator ou não utiliza. Essa objetividade facilita o trabalho de auditoria e reduz disputas sobre interpretação.

Seguradoras de riscos cibernéticos utilizam o CIS Controls como base para questionários de subscrição. A lógica é atuarial: organizações que implementam os controles têm menor probabilidade de sofrer incidentes graves e, portanto, representam menor risco para a seguradora. Muitas apólices de seguro cibernético condicionam cobertura ou valores de prêmio à demonstração de que determinados controles estão implementados. O IG1 do CIS Controls frequentemente aparece como baseline mínimo esperado.

Reguladores, mesmo quando não mencionam explicitamente o CIS Controls em suas normas, utilizam-no como referência implícita do que constitui "medidas técnicas e administrativas adequadas". A LGPD, em seu artigo 46, exige que agentes de tratamento adotem tais medidas para proteger dados pessoais, mas não especifica quais medidas. O CIS Controls oferece uma resposta concreta a essa exigência: são estas as medidas que a comunidade internacional de segurança considera adequadas.

O Community Defense Model (CDM)[5], publicado pelo CIS, reforça essa credibilidade com dados. Segundo a análise do CDM versão 2.0, a implementação completa do IG1 (as 56 salvaguardas essenciais) defende contra 74% das técnicas documentadas no MITRE ATT&CK. Esse número oferece uma métrica objetiva do valor defensivo do framework: não é marketing nem opinião, é correlação demonstrável entre controles implementados e ataques bloqueados.

[5] CENTER FOR INTERNET SECURITY. CIS introduces v2.0 of the CIS Community Defense Model. 2021. Disponível em: https://www.cisecurity.org/insights/blog/cis-introduces-v2-0-of-the-cis-community-defense-model - Acesso em jan. 2026.

O CIS Controls como Limite de Tolerância à Negligência

Chegamos ao ponto que justifica a epígrafe deste livro: o CIS Controls não é apenas um framework de segurança; é, na prática, um framework de responsabilidade.

Essa afirmação requer explicação. Em um mundo onde ataques cibernéticos são cotidianos e suas consequências podem incluir vazamento de dados pessoais, interrupção de operações, perdas financeiras e danos reputacionais, a pergunta que reguladores, tribunais e a opinião pública fazem após um incidente é: a organização fez o que deveria ter feito?

O CIS Controls oferece uma resposta a essa pergunta. Uma organização que implementa o IG1 pode demonstrar que adotou o que a comunidade internacional de segurança considera o mínimo essencial. Uma organização que vai além, implementando IG2 ou IG3, demonstra maturidade adicional proporcional a seu perfil de risco. A documentação dessa implementação transforma intenções em evidências.

Por outro lado, uma organização que sofre um incidente e não consegue demonstrar implementação de controles básicos enfrenta uma situação difícil. A pergunta "por que vocês não tinham inventário de ativos?" ou "por que não utilizavam autenticação multifator?" não tem resposta satisfatória quando o framework que recomenda essas medidas está disponível gratuitamente há quase duas décadas.

O CIS Controls, portanto, estabelece um limite de tolerância à negligência. Abaixo desse limite, a organização assume riscos que transcendem o técnico e entram no território do jurídico. A ausência de controles básicos deixa de ser uma escolha técnica e passa a ser uma exposição a responsabilização.

Esse é o tema que desenvolveremos nos capítulos seguintes: como o CIS Controls se traduz em instrumento de governança, como se relaciona com a LGPD e outras regulamentações, e como pode ser implementado de forma proporcional por organizações de diferentes portes e perfis de risco.

Referências do capítulo

CENTER FOR INTERNET SECURITY. CIS Critical Security Controls Version 8.1. East Greenbush: CIS, 2024. Disponível em: https://www.cisecurity.org/controls/v8-1. Acesso em: 15 jan. 2026.

CENTER FOR INTERNET SECURITY. CIS Community Defense Model v2.0. East Greenbush: CIS, 2022. Disponível em: https://www.cisecurity.org/insights/white-papers/cis-community-defense-model-2-0. Acesso em: 15 jan. 2026.

CENTER FOR INTERNET SECURITY. Guide to Implementation Groups (IG): CIS Critical Security Controls v8.1. East Greenbush: CIS, 2024. Disponível em: https://www.cisecurity.org/controls/v8-1. Acesso em: 15 jan. 2026.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 15 jan. 2026.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. NIST Cybersecurity Framework 2.0. Gaithersburg: NIST, 2024. Disponível em: https://www.nist.gov/cyberframework. Acesso em: 15 jan. 2026.

MITRE CORPORATION. MITRE ATT&CK Framework. McLean: MITRE, 2024. Disponível em: https://attack.mitre.org/. Acesso em: 15 jan. 2026.

CAPÍTULO 2 - Por que o CIS v8.1 mudou o jogo

O Framework Consolidado

Quando uma organização decide estruturar sua postura de segurança da informação, encontra pela frente um universo de opções. Frameworks, normas, regulamentações, certificações, metodologias proprietárias de consultorias, recomendações de fabricantes de tecnologia. A quantidade de informação disponível pode ser tão paralisante quanto a ausência dela. Nesse cenário, o CIS Controls v8.1 representa algo incomum: um framework que chegou à maturidade sem perder acessibilidade.

A versão 8.1, publicada em junho de 2024, não é resultado de exercício teórico nem de comitê de padronização distante da realidade operacional. É produto de quase duas décadas de refinamento contínuo, alimentado por dados de incidentes reais, feedback de profissionais que implementam os controles em ambientes diversos, e análise sistemática das técnicas utilizadas por adversários. Cada iteração do framework incorporou lições aprendidas da versão anterior, removendo redundâncias, clarificando ambiguidades, e ajustando prioridades conforme o cenário de ameaças evoluiu.

Para o leitor que chega ao CIS Controls pela primeira vez, essa história evolutiva importa menos do que a arquitetura atual. O que interessa é compreender como o framework está organizado e por que essa organização facilita decisões de negócio, não apenas decisões técnicas.

Arquitetura do Framework: 18 Controles, 153 Salvaguardas

O CIS Controls v8.1 didaticamente, estrutura-se em dois níveis hierárquicos. No nível superior estão 18 Controles de alto nível para governança, cada um representando um domínio de segurança. Dentro de cada Controle estão as Salvaguardas (Safeguards), que totalizam 153 ações específicas e mensuráveis.

Os 18 Controles cobrem o espectro de capacidades defensivas que uma organização precisa desenvolver. Os dois primeiros tratam de inventário (o que existe na organização). O terceiro aborda proteção de dados. O quarto trata de configuração segura. Os Controles 5 e 6 endereçam gestão de contas e controle de acesso. O Controle 7 foca gestão de vulnerabilidades. O Controle 8 aborda gestão de registros de auditoria (logs). O Controle 9 trata de proteções para e-mail e navegação web. O Controle 10 endereça defesas contra malware. O Controle 11 aborda recuperação de dados. Os Controles 12 e 13 tratam de infraestrutura e monitoramento de rede. O Controle 14 endereça conscientização e treinamento. O Controle 15 trata de gestão

de provedores de serviço. O Controle 16 aborda segurança de software aplicativo. O Controle 17 trata de resposta a incidentes. O Controle 18 foca testes de penetração.

Cada uma das 153 Salvaguardas é associada a três dimensões que facilitam priorização e implementação: um Tipo de Ativo (Asset Type), uma Função de Segurança (Security Function) e um ou mais Grupos de Implementação (Implementation Groups).

Tipos de Ativos: Onde as Salvaguardas se Aplicam

O CIS Controls v8.1 define seis Tipos de Ativos que refletem os diferentes componentes do ambiente organizacional onde as medidas de proteção devem ser aplicadas:

Dispositivos (Devices) compreendem os ativos de hardware: servidores, estações de trabalho, notebooks, equipamentos de rede, dispositivos móveis, equipamentos IoT (Internet das Coisas).

Softwares (Software) abrangem os aplicativos, sistemas operacionais, bibliotecas e componentes de software instalados nos dispositivos.

Dados (Data) referem-se às informações que a organização armazena, processa e transmite, independentemente do formato ou localização.

Usuários (Users) representam as identidades humanas e não humanas[6] que interagem com os sistemas organizacionais, incluindo suas credenciais, permissões e comportamentos.

Redes (Networks) compreendem a infraestrutura de comunicação que conecta os demais elementos: redes locais, redes remotas, conexões com a internet, segmentos de rede.

Documentação (Documentation), adicionada na versão 8.1, abrange planos, políticas, procedimentos e processos documentados que suportam o programa de segurança.

Essa classificação permite que organizações identifiquem rapidamente quais salvaguardas são relevantes para cada componente de seu ambiente. Uma salvaguarda relacionada a Dispositivos, por exemplo, aplica-se à gestão de hardware; uma relacionada a Documentação aplica-se a políticas e procedimentos formalizados.

[6] Identidades humanas são características indivíduais (senhas, autenticação multifator (MFA) e biometria, etc.), enquanto identidades não humanas (NHIs) são digitais, pertencentes a máquinas, aplicativos e processos automatizados, usadas para comunicação e tarefas de TI, autenticadas via tokens/chaves de API, e representam um desafio de segurança por sua escala e menor controle.

Funções de Segurança: Alinhamento com NIST CSF 2.0

Cada Salvaguarda no CIS Controls v8.1 é mapeada a uma das seis Funções de Segurança, alinhadas ao NIST Cybersecurity Framework 2.0:

Identificar (Identify) agrupa salvaguardas relacionadas a compreender o ambiente organizacional, os ativos, os riscos e as capacidades existentes.

Proteger (Protect) agrupa salvaguardas que estabelecem medidas preventivas para limitar ou conter o impacto de potenciais eventos de segurança.

Detectar (Detect) agrupa salvaguardas relacionadas a descobrir a ocorrência de eventos de segurança de forma tempestiva.

Responder (Respond) agrupa salvaguardas que endereçam a capacidade de agir quando um evento de segurança é detectado.

Recuperar (Recover) agrupa salvaguardas relacionadas a restaurar capacidades e serviços afetados por um evento de segurança.

Governar (Govern), adicionada na versão 8.1 para alinhamento com o NIST CSF 2.0, agrupa salvaguardas que estabelecem estruturas de governança para o programa de segurança.

Essa classificação permite que organizações avaliem sua postura de segurança de forma equilibrada, identificando se há concentração excessiva em uma função (tipicamente Proteger) e lacunas em outras (tipicamente Detectar e Responder).

Por Que Salvaguardas e Não sub-controles

O termo "salvaguarda" (safeguard) substituiu "sub-control" a partir da versão 8 do framework. Essa mudança terminológica não é cosmética; carrega implicações conceituais significativas.

De forma didática o termo "controle" evoca mecanismo de verificação, de comando, de fiscalização. Sugere algo que se instala, se configura e passa a funcionar automaticamente. Essa conotação pode induzir a uma compreensão equivocada: a de que segurança consiste em implementar mecanismos técnicos que, uma vez ativados, operam sem intervenção adicional.

O termo "salvaguarda" evoca medida preventiva, proteção antecipada, cuidado deliberado. Uma salvaguarda é uma ação tomada antecipadamente para proteger algo valioso ou mitigar um risco identificado. O conceito implica que a organização está consciente do risco e adota medidas específicas para endereçá-lo.

Há uma distinção importante entre salvaguarda e controle que merece ser explicitada: a salvaguarda vem primeiro, o controle vem depois. Primeiro a organização implementa as salvaguardas, medidas preventivas que estabelecem

proteções. Depois a organização controla, ou seja, verifica se as salvaguardas estão operando conforme esperado, produzindo evidências de sua eficácia.

Considere um exemplo concreto. A Salvaguarda 11.2 prescreve "Perform Automated Backups" (Realizar Backups Automatizados). A organização implementa essa salvaguarda configurando rotinas de backup automatizado. O controle vem depois: verificar periodicamente se os backups estão sendo executados conforme programado, se os dados estão íntegros, se a restauração funciona quando testada. A salvaguarda é a medida de proteção; o controle é a verificação de que a medida funciona.

Essa distinção tem relevância prática. Organizações que confundem salvaguarda com controle frequentemente instalam mecanismos técnicos e os consideram implementados, sem estabelecer processos de verificação contínua. Meses depois descobrem que o backup não funcionava, que o antivírus estava desatualizado, que as contas órfãs se acumularam. A salvaguarda existia no papel; o controle que garantiria sua eficácia nunca foi estabelecido.

Implementation Groups: Segurança Proporcional

Se o CIS Controls parasse na lista de 153 salvaguardas, seria útil como referência técnica, mas problemático como guia de implementação. A pergunta inevitável de qualquer gestor seria: por onde começar? Fazer tudo simultaneamente é impossível para qualquer organização. Fazer em ordem numérica não necessariamente reflete prioridades de risco.

A resposta do framework são os Implementation Groups (Grupos de Implementação), designados como IG1, IG2 e IG3. Essa estratificação representa uma das contribuições mais valiosas do CIS Controls para organizações de qualquer porte.

Implementation Group 1 (IG1) é o que o CIS denomina "higiene cibernética essencial" (essential cyber hygiene). Contém 56 salvaguardas que a comunidade de segurança considera o “mínimo absoluto” para qualquer organização, independentemente de porte, setor ou complexidade. Essas 56 salvaguardas foram selecionadas com base em dois critérios: eficácia demonstrada contra os ataques mais comuns e viabilidade de implementação com recursos limitados.

Cinquenta e seis salvaguardas podem parecer muito. Na realidade, são muito pouco quando comparadas à totalidade de 153 salvaguardas do framework ou às centenas de requisitos de normas como ISO 27001. As 56 salvaguardas do IG1 representam o essencial destilado, o núcleo irredutível, o mínimo abaixo do qual não se pode alegar cuidado razoável.

Segundo análises publicadas pelo CIS no Community Defense Model v2.0, a implementação completa do IG1 defende contra 74% das técnicas documentadas no MITRE ATT&CK. Esse dado merece ser absorvido: menos de 40% das salvaguardas

totais do framework proporcionam proteção contra quase três quartos das técnicas conhecidas de ataque.

Implementation Group 2 (IG2) adiciona 74 salvaguardas ao IG1, totalizando 130. Destina-se a organizações que gerenciam infraestrutura tecnológica mais complexa, que operam em ambientes regulados, ou que processam dados de maior sensibilidade. As salvaguardas do IG2 frequentemente requerem expertise especializada para implementação e ferramentas de categoria empresarial.

Implementation Group 3 (IG3) incorpora as 23 salvaguardas restantes, completando as 153 do framework. Destina-se a organizações de grande porte, alta complexidade operacional, exposição significativa a ameaças sofisticadas, ou requisitos regulatórios rigorosos.

A lógica dos Implementation Groups é cumulativa: IG2 inclui todas as salvaguardas do IG1, e IG3 inclui todas as salvaguardas do IG1 e IG2. Uma organização não "escolhe" um grupo; ela progride através deles conforme sua maturidade e necessidades evoluem. E, crucialmente, toda organização começa pelo IG1. Não há atalho que permita pular a higiene básica em direção a capacidades avançadas.

O Ecossistema CIS: Além dos Controls

O CIS Controls não existe isoladamente. Faz parte de um ecossistema de recursos desenvolvidos pelo Center for Internet Security para apoiar organizações em diferentes estágios de maturidade e com diferentes necessidades. Compreender esse ecossistema ajuda a posicionar o framework no contexto mais amplo e a identificar recursos complementares.

CIS Controls são o que discutimos neste livro: a lista priorizada de 18 controles e 153 salvaguardas que estabelecem o que uma organização deveria fazer para proteger-se contra ameaças cibernéticas comuns. Os Controls respondem à pergunta "o quê fazer?"

CIS Benchmarks são guias de configuração segura para mais de 100 tecnologias específicas, abrangendo sistemas operacionais, plataformas de nuvem, dispositivos de rede, aplicativos de desktop, servidores de banco de dados e outras categorias. Os Benchmarks respondem à pergunta "como configurar?" Enquanto o CIS Controls prescreve, por exemplo, "estabelecer configuração segura para ativos corporativos" (Controle 4), o CIS Benchmark para Windows Server 2022 detalha exatamente quais configurações devem ser aplicadas nesse sistema operacional específico. Os dois recursos são complementares: Controls indicam a direção, Benchmarks fornecem o mapa detalhado.

CIS RAM (Risk Assessment Method) é uma metodologia de avaliação de risco desenvolvida em parceria com a HALOCK Security Labs. O CIS RAM ajuda

organizações a definir seu nível aceitável de risco e a justificar investimentos na implementação dos CIS Controls de forma proporcional. A versão atual, CIS RAM v2.1, oferece três abordagens diferentes para organizações com diferentes níveis de maturidade, alinhadas aos Implementation Groups. O CIS RAM é particularmente valioso porque incorpora princípios do padrão DoCRA (Duty of Care Risk Analysis), que alinha a análise de risco de segurança da informação aos conceitos de "dever de cuidado" e "cuidado razoável" utilizados por tribunais e reguladores.

CIS CSAT (Controls Self-Assessment Tool) é uma ferramenta de autoavaliação que permite às organizações acompanhar e priorizar sua implementação dos CIS Controls. A versão hospedada pelo CIS (CIS-Hosted CSAT) está disponível gratuitamente para uso não comercial. A ferramenta permite que equipes colaborem na avaliação, gerem relatórios executivos, e comparem anonimamente seus resultados com a média de seu setor. Para organizações que necessitam de recursos adicionais, existe o CIS CSAT Pro, disponível para membros do CIS SecureSuite.

Esses quatro componentes formam um ciclo virtuoso: os Controls estabelecem o que fazer, os Benchmarks detalham como configurar, o RAM permite avaliar e priorizar riscos, e o CSAT permite medir e acompanhar o progresso. Organizações podem utilizar cada componente independentemente, mas obtêm maior valor quando os utilizam de forma integrada.

Todos estão disponíveis gratuitamente.

Por Que o CIS Funciona para PMEs

Um argumento frequente contra frameworks de segurança é que foram desenhados para grandes corporações com orçamentos dedicados e equipes especializadas. Pequenas e médias empresas, segundo esse argumento, não conseguem implementar frameworks complexos porque não dispõem dos recursos necessários.

O CIS Controls v8.1, particularmente através do IG1, refuta esse argumento. O grupo foi explicitamente desenhado para ser implementável por organizações com expertise limitada em segurança cibernética, utilizando processos e tecnologias que tipicamente já estão disponíveis ou que podem ser adquiridas a custo acessível.

O IG1 contempla explicitamente a realidade de que muitas organizações menores terceirizam suas necessidades de tecnologia para provedores de serviços gerenciados (MSPs), provedores de serviços em nuvem (CSPs) ou provedores de serviços gerenciados de segurança (MSSPs). As salvaguardas são formuladas de forma que possam ser implementadas diretamente pela organização ou delegadas a fornecedores, desde que a organização mantenha visibilidade e supervisão adequadas.

A premissa do IG1 é que segurança básica não é privilégio de quem tem recursos abundantes. É necessidade de qualquer organização que opera em ambiente digital, e deve ser alcançável por qualquer organização disposta a fazer o esforço.

Segurança Proporcional versus Segurança Idealizada

Chegamos ao ponto que talvez mais diferencie o CIS Controls de abordagens concorrentes: a recusa explícita da segurança idealizada em favor da segurança proporcional.

Frameworks de segurança podem operar de duas formas. Podem descrever um estado ideal de proteção, deixando para cada organização determinar como e quanto desse ideal implementar. Ou podem oferecer orientação estratificada que reconhece diferentes realidades organizacionais e diferentes níveis de maturidade aceitáveis.

A primeira abordagem tem apelo intelectual: apresenta a imagem completa do que seria a segurança tendendo a ser perfeita. Mas frequentemente paralisa organizações menores, que olham para a totalidade do que "deveriam" fazer e concluem que é impossível, optando por não fazer nada. O perfeito torna-se inimigo do adequado.

O CIS Controls adota a segunda abordagem. Ao estratificar salvaguardas em Implementation Groups, o framework comunica explicitamente que nem toda organização precisa implementar tudo. Comunica que existe um mínimo aceitável (IG1) que qualquer organização pode e deve alcançar. Comunica que a progressão para níveis superiores é desejável, mas não obrigatória para todos. Comunica que segurança é jornada incremental, não destino binário.

Essa proporcionalidade também encerra um argumento frequentemente utilizado como desculpa para inação: "segurança é cara demais". O IG1 demonstra que o mínimo defensável não é caro demais. É acessível para praticamente qualquer organização que opere formalmente. O que é caro demais é sofrer um incidente grave sem ter implementado sequer o básico.

O Fim da Desculpa

Ao longo de quase duas décadas, o CIS Controls evoluiu de uma lista informal de recomendações para um framework maduro, estratificado, validado por dados e adotado globalmente como referência de diligência em segurança da informação. A versão 8.1 representa o estado atual dessa evolução: consolidada o suficiente para ser confiável, flexível o suficiente para ser aplicável a contextos diversos, específica o suficiente para ser implementável.

O ecossistema que circunda os Controls (Benchmarks, RAM, CSAT) oferece recursos complementares para organizações que desejam não apenas saber o que fazer, mas também como fazer, como priorizar e como medir progresso. Todos esses recursos estão disponíveis gratuitamente para uso não comercial.

Para executivos, gestores e profissionais que buscavam um ponto de partida claro para estruturar a segurança de suas organizações, o CIS Controls oferece exatamente isso. A estratificação em Implementation Groups remove a desculpa de que segurança é inacessível para organizações menores. As 56 salvaguardas do IG1 definem um mínimo defensável que qualquer organização pode alcançar, e a proteção contra 74% das técnicas de ataque conhecidas que esse mínimo proporciona demonstra que fazer pouco é infinitamente melhor que fazer nada.

A pergunta que resta não é mais "o que fazer?" O CIS Controls responde essa pergunta com clareza considerável. A pergunta que resta é "por que ainda não fizemos?" E essa pergunta, como veremos nos capítulos seguintes, tem implicações que transcendem o técnico e adentram o território da responsabilidade.

Referências do Capítulo

CENTER FOR INTERNET SECURITY. CIS Critical Security Controls Version 8.1. East Greenbush: CIS, 2024. Disponível em: https://www.cisecurity.org/controls/v8-1. Acesso em: 15 jan. 2026.

CENTER FOR INTERNET SECURITY. Guide to Asset Classes: CIS Critical Security Controls v8.1. East Greenbush: CIS, 2024. Disponível em: https://www.cisecurity.org/insights/white-papers/guide-to-asset-classes-cis-critical-security-controls-v8-1. Acesso em: 15 jan. 2026.

CENTER FOR INTERNET SECURITY. CIS Benchmarks. East Greenbush: CIS, 2024. Disponível em: https://www.cisecurity.org/cis-benchmarks. Acesso em: 15 jan. 2026.

CENTER FOR INTERNET SECURITY. CIS RAM (Risk Assessment Method). East Greenbush: CIS, 2022. Disponível em: https://www.cisecurity.org/insights/white-papers/cis-ram-risk-assessment-method. Acesso em: 15 jan. 2026.

CENTER FOR INTERNET SECURITY. CIS Risk Assessment Method (RAM) v2.1 for CIS Controls v8. East Greenbush: CIS, 2022. Disponível em: https://www.cisecurity.org/insights/blog/cis-risk-assessment-method-ram-v2-1-for-cis-controls-v8. Acesso em: 15 jan. 2026.

CENTER FOR INTERNET SECURITY. CIS-Hosted CSAT: A Free Tool for Assessing Implementation of CIS Critical Security Controls. East Greenbush: CIS, 2021. Disponível em: https://www.cisecurity.org/insights/blog/cis-csat-free-tool-assessing-implementation-of-cis-controls. Acesso em: 15 jan. 2026.

CENTER FOR INTERNET SECURITY. CIS Controls Self Assessment Tool (CSAT). East Greenbush: CIS, 2024. Disponível em: https://www.cisecurity.org/controls/cis-controls-self-assessment-tool-cis-csat. Acesso em: 15 jan. 2026.

CENTER FOR INTERNET SECURITY. CIS Community Defense Model v2.0. East Greenbush: CIS, 2022. Disponível em: https://www.cisecurity.org/insights/white-papers/cis-community-defense-model-2-0. Acesso em: 15 jan. 2026.

MITRE CORPORATION. MITRE ATT&CK Framework. McLean: MITRE, 2024. Disponível em: https://attack.mitre.org/. Acesso em: 15 jan. 2026.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. NIST Cybersecurity Framework 2.0. Gaithersburg: NIST, 2024. Disponível em: https://www.nist.gov/cyberframework. Acesso em: 15 jan. 2026.

PARTE II: O CIS Control como Instrumento de Decisão

CAPÍTULO 3 - Diligência Razoável e Responsabilidade

3.1 O Conceito Jurídico de Diligência Razoável Aplicado à Segurança da Informação

A expressão "diligência razoável" atravessa séculos de tradição jurídica ocidental, originando-se no conceito romano de *bonus pater familias*, o administrador prudente que cuida dos interesses alheios como cuidaria dos próprios. Transportado para o direito empresarial contemporâneo, esse padrão de conduta tornou-se pedra angular na avaliação da responsabilidade de gestores, conselheiros e organizações perante stakeholders (partes interessadas), reguladores e tribunais.

No contexto da segurança da informação, diligência razoável não significa perfeição. Nenhum sistema é absolutamente seguro, e nenhum regulador ou tribunal razoável espera que seja. O que se exige é demonstração objetiva de que a organização adotou medidas proporcionais aos riscos conhecidos, compatíveis com sua capacidade econômica e alinhadas às melhores práticas reconhecidas pelo setor.

A questão que magistrados, auditores e reguladores formulam após um incidente não é "por que o ataque teve sucesso?", pois ataques sofisticados eventualmente terão sucesso contra qualquer defesa. A pergunta determinante é outra: o que a organização fez antes do incidente para preveni-lo ou mitigar suas consequências?

Essa distinção é fundamental. O direito não pune o resultado adverso em si, mas a conduta que o precedeu. Uma organização que sofre vazamento de dados após implementar controles reconhecidos, treinar colaboradores, monitorar sistemas e manter planos de resposta documentados encontra-se em posição jurídica radicalmente diferente daquela que operava sem qualquer estrutura defensiva. A primeira demonstra diligência. A segunda, negligência.

O padrão de diligência razoável em segurança cibernética cristalizou-se progressivamente através de decisões regulatórias, jurisprudência internacional e consenso técnico. Organizações como o Center for Internet Security (CIS), o National Institute of Standards and Technology (NIST) e a International Organization for Standardization (ISO) desenvolveram frameworks (modelos de referência estruturados) que, embora tecnicamente voluntários, tornaram-se referências implícitas do que constitui cuidado adequado. Ignorar completamente essas orientações quando disponíveis e acessíveis, a maioria sem custos, configura em muitas jurisdições, presunção de negligência.

O conceito opera em duas dimensões complementares.

A primeira é substantiva: a organização efetivamente implementou medidas de proteção?

A segunda é probatória: a organização consegue demonstrar documentalmente o que implementou?

Muitas organizações falham na segunda dimensão mesmo quando razoavelmente bem-sucedidas na primeira. Controles existem, mas não há registros. Políticas foram comunicadas, mas não há evidência de ciência. Treinamentos ocorreram, mas não há listas de presença. Essa lacuna documental transforma diligência real em negligência aparente quando chega o momento de prestar contas.

3.2 CIS Controls como Demonstração Objetiva de Cuidado

Quando um regulador, auditor ou magistrado avalia a postura de segurança de uma organização, enfrenta um desafio epistemológico: como um não-especialista pode determinar se as medidas adotadas eram adequadas? A resposta prática reside em referenciais externos reconhecidos. Se a organização demonstra alinhamento com framework aceito pela comunidade técnica e regulatória, estabelece-se presunção favorável de adequação. Se opera sem qualquer referencial, o ônus de provar que suas medidas “ad hoc” (improvisadas para a situação específica) eram suficientes recai inteiramente sobre ela.

O CIS Controls ocupa posição privilegiada nesse ecossistema de referenciais. Diferentemente de frameworks mais abstratos ou extensos, as mediadas e controles foram desenhados para implementação prática, com linguagem acessível e priorização clara. Os dezoito controles e suas cento e cinquenta e três salvaguardas representam consenso de centenas de especialistas sobre o que efetivamente funciona para prevenir ataques reais. Não se trata de construção teórica, mas de destilação de experiência operacional.

Essa característica confere aos CIS Controls força argumentativa singular em contextos de prestação de contas. Quando uma organização demonstra que implementou os controles do “Implementation Group 1” (IG1), o conjunto mínimo recomendado para qualquer organização, estabelece linha de base defensável. Quando avança para IG2 ou IG3, demonstra maturidade progressiva proporcional à sensibilidade de seus ativos e à sofisticação de suas operações.

A estrutura dos CIS Controls facilita ainda a comunicação entre domínios tradicionalmente isolados. Executivos compreendem a lógica de priorização baseada em risco. Advogados reconhecem a correspondência com requisitos regulatórios. Auditores encontram controles verificáveis e mensuráveis. Técnicos identificam implementações concretas. Essa traduzibilidade entre linguagens profissionais é rara em frameworks de segurança e particularmente valiosa quando múltiplos stakeholders precisam avaliar a mesma realidade.

Tribunais e reguladores em jurisdições diversas têm progressivamente reconhecido frameworks como os CIS Controls como evidência de diligência.

A Federal Trade Commission (FTC, comissão federal de comércio norte-americana), em diversas ações de enforcement (aplicação de sanções), referenciou explicitamente a ausência de controles básicos, como inventário de ativos, gestão de vulnerabilidades e controle de acesso, como indicadores de práticas inadequadas. O Information Commissioner's Office (ICO, autoridade britânica de proteção de dados), ao aplicar sanções sob o GDPR (General Data Protection Regulation, regulamento europeu de proteção de dados), frequentemente analisa se a organização mantinha medidas alinhadas a padrões reconhecidos. A tendência é inequívoca: frameworks técnicos consensuais estão se tornando o metro pelo qual se mede a diligência organizacional.

3.3 Relação Direta com a LGPD: Medidas Técnicas e Administrativas Adequadas

A Lei Geral de Proteção de Dados brasileira estabelece, em seu Artigo 46, que agentes de tratamento devem adotar "medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito." O dispositivo é deliberadamente principiológico. Não prescreve tecnologias específicas nem enumera controles obrigatórios. Essa abertura, característica de legislações modernas de proteção de dados, transfere ao agente de tratamento a responsabilidade de determinar o que constitui "medidas aptas" em seu contexto específico.

A indeterminação do conceito legal cria simultaneamente flexibilidade e risco. Flexibilidade porque permite adaptação a diferentes portes, setores e perfis de risco. Risco porque, na ausência de orientação regulamentar detalhada, a organização pode descobrir somente após um incidente que suas medidas eram consideradas insuficientes. A adoção de framework reconhecido como os CIS Controls mitiga esse risco ao ancorar decisões organizacionais em consenso técnico externo.

A correspondência entre os CIS Controls e as exigências implícitas do Art. 46 é notavelmente direta. O Controle 1 (Inventário e Controle de Ativos Corporativos) e o Controle 2 (Inventário e Controle de Ativos de Software) respondem à necessidade básica de conhecer o que se protege, premissa lógica de qualquer programa de segurança. O Controle 3 (Proteção de Dados) mapeia diretamente para a proteção contra "acessos não autorizados" e "situações acidentais de destruição, perda, alteração." O Controle 4 (Configuração Segura) e o Controle 7 (Gestão Contínua de Vulnerabilidades) endereçam a prevenção de "tratamento inadequado ou ilícito" decorrente de falhas técnicas evitáveis.

O Artigo 46 menciona expressamente medidas "administrativas" além das técnicas. Os CIS Controls contemplam essa dimensão através de controles como o 14 (Conscientização e Treinamento em Segurança), o 15 (Gestão de Provedores de Serviços) e o 17 (Gestão de Resposta a Incidentes). A Lei não distingue entre falhas

técnicas e humanas; ambas podem configurar violação. Uma organização que implementa firewalls sofisticados, mas não treina colaboradores sobre phishing (golpe de engenharia social por e-mail ou mensagem) deixa flanco aberto que os CIS Controls explicitamente endereçam.

A Agência Nacional de Proteção de Dados, embora ainda em processo de evolução, já sinalizou em documentos orientativos a expectativa de que organizações adotem frameworks reconhecidos. O Guia Orientativo sobre Segurança da Informação para Agentes de Tratamento de Pequeno Porte, publicado pela ANPD, recomenda medidas como inventário de ativos/dados, controle de acesso, cópias de segurança e atualização de sistemas, que coincidem em grande parte com as salvaguardas de baseline do Implementation Group 1 dos CIS Controls, refletindo o consenso internacional sobre uma linha de base razoável de segurança.

Um ponto crítico permanece em aberto. O Artigo 46, parágrafo primeiro, prevê que a ANPD "poderá dispor sobre padrões técnicos mínimos" de segurança. Até janeiro de 2026, esse dispositivo não foi regulamentado, o que mantém o conceito de "medidas adequadas" relativamente indeterminado. Especialistas apontam que essa ausência de critérios dificulta tanto a fiscalização quanto a defesa das organizações. A adoção proativa de frameworks como os CIS Controls preenche parcialmente essa lacuna, oferecendo referencial objetivo enquanto a regulamentação não se materializa.

3.4 O CIS como Resposta à Pergunta do Regulador Pós-Incidente

Incidentes de segurança são inevitáveis. A questão não é se ocorrerão, mas quando, e como a organização responderá tanto tecnicamente quanto perante reguladores. No Brasil, a LGPD estabelece obrigação de comunicação à ANPD e, em determinados casos, aos titulares afetados. Essa comunicação desencadeia escrutínio regulatório que pode resultar em sanções administrativas significativas, incluindo multas de até dois por cento do faturamento, limitadas a cinquenta milhões de reais por infração.

A análise regulatória pós-incidente tipicamente percorre três eixos. Primeiro: a organização mantinha medidas preventivas adequadas antes do incidente? Segundo: a organização detectou o incidente em tempo razoável? Terceiro: a organização respondeu apropriadamente após a detecção? Os CIS Controls fornecem estrutura para responder afirmativamente aos três eixos.

No primeiro eixo, a existência de programa de segurança baseado em CIS Controls demonstra investimento sistemático em prevenção. Não se trata de apresentar ao regulador uma lista de tecnologias adquiridas, mas de evidenciar processo contínuo de gestão de risco. Políticas documentadas, controles implementados, exceções registradas e justificadas, revisões periódicas. Esse conjunto probatório transforma alegação em demonstração.

No segundo eixo, o Controle 8 (Gestão de Registros de Auditoria) e o Controle 13 (Monitoramento e Defesa de Rede) estabelecem capacidade de detecção. O regulador perguntará: vocês tinham visibilidade sobre o que acontecia em seus sistemas? Os logs (registros de eventos) existiam e eram analisados? Havia alertas configurados para comportamentos anômalos? Organizações que implementam esses controles podem demonstrar que, mesmo quando a prevenção falhou, mantinham capacidade de identificar a falha.

No terceiro eixo, o Controle 17 (Gestão de Resposta a Incidentes) fornece arcabouço para ação coordenada. Plano de resposta documentado, equipe designada, procedimentos de contenção, comunicação estruturada. Esses elementos demonstram que a organização não improvisou sob pressão, mas executou processo previamente definido. O regulador distingue claramente entre organizações que responderam caoticamente e aquelas que ativaram protocolos estabelecidos.

A documentação assume papel central nesse contexto. Não basta ter implementado controles; é necessário poder provar a implementação. Registros de configuração, evidências de treinamento, relatórios de vulnerabilidades corrigidas, atas de comitês de segurança, resultados de testes de penetração. Esse acervo documental constitui a defesa da organização.

Os CIS Controls, através do CIS Controls Assessment Specification (CIS CSAT, ferramenta de autoavaliação de maturidade), oferecem metodologia padronizada para documentar níveis de implementação, facilitando tanto a gestão interna quanto a prestação de contas externa.

A Resolução CD/ANPD nº 15/2024 estabeleceu que a comunicação de incidentes deve ocorrer em até três dias úteis após a confirmação do evento, podendo ser prorrogada por até vinte dias quando necessário. Para que haja obrigação de comunicação, deve estar presente "dano ou risco relevante" aos titulares. Organizações que mantêm registros estruturados segundo os CIS Controls conseguem avaliar mais rapidamente a extensão do incidente e fundamentar suas decisões de comunicação em evidências objetivas.

3.5 O que o Juiz, o Auditor e o Segurador Esperam Encontrar

Três figuras distintas, o magistrado em litígio civil, o auditor em verificação de conformidade e o subscritor de apólice cyber, compartilham necessidade comum: avaliar se a organização agiu com prudência proporcional aos riscos que enfrentava. Cada um opera em contexto próprio, com critérios específicos, mas convergem na busca por evidências objetivas de diligência.

O magistrado, em ação de responsabilidade civil decorrente de incidente de segurança, aplica o padrão do homem médio ou, mais precisamente, do gestor médio em circunstâncias similares. A pergunta implícita é: uma organização razoável, do mesmo porte e setor, teria adotado as mesmas medidas ou medidas superiores? Se

a resposta for negativa, configura-se negligência. Se positiva, o dano ocorrido não decorre de culpa, mas de risco inerente à atividade.

A demonstração de alinhamento com CIS Controls posiciona a organização favoravelmente nessa análise comparativa. Não se trata de imunidade, pois responsabilidade objetiva pode existir independentemente de culpa, mas de defesa robusta contra alegações de negligência.

O auditor, seja interno, externo ou regulatório, opera com metodologia estruturada. Busca evidências de controles, testa sua efetividade, documenta lacunas. Frameworks como os CIS Controls facilitam esse trabalho ao fornecer taxonomia comum. O auditor não precisa inventar critérios; aplica referencial reconhecido. Organizações que já estruturaram sua segurança segundo CIS Controls falam a mesma linguagem do auditor, reduzindo fricção e ambiguidade. O relatório resultante reflete maturidade demonstrável, não alegações vagas de "levamos segurança a sério."

O subscritor de seguro cyber realiza análise de risco para precificação. Quanto maior o risco percebido, maior o prêmio ou, em casos extremos, a recusa de cobertura. Seguradoras desenvolveram questionários extensos que, em sua essência, mapeiam para controles fundamentais: vocês mantêm inventário de ativos? Implementam autenticação multifator (MFA, verificação de identidade em duas ou mais etapas)? Realizam backups testados? Treinam colaboradores?

A convergência com os CIS Controls é evidente. Organizações que podem responder afirmativamente, com evidências, obtêm condições mais favoráveis. Mais importante: em caso de sinistro, a demonstração de controles implementados fortalece a posição da organização contra alegações de violação de garantias contratuais que poderiam comprometer a cobertura.

Os três stakeholders compartilham ainda expectativa de proporcionalidade. Uma startup de cinco pessoas não precisa implementar o mesmo nível de controles que uma instituição financeira sistêmica. Os CIS Controls, através dos Implementation Groups (grupos de implementação graduados por maturidade), incorporam essa proporcionalidade. IG1 representa o mínimo para qualquer organização. IG2 adiciona controles para organizações com dados sensíveis ou infraestrutura crítica. IG3 contempla organizações que enfrentam adversários sofisticados. Essa graduação permite que cada organização demonstre diligência proporcional ao seu contexto.

3.6 Responsabilidade Pessoal de Executivos e Conselheiros

A responsabilização pessoal de administradores por falhas de segurança cibernética deixou de ser hipótese teórica para tornar-se realidade jurídica em múltiplas jurisdições. No Brasil, o Código Civil estabelece que administradores respondem por atos praticados com culpa ou dolo, ou com violação da lei ou do estatuto. A Lei das Sociedades por Ações detalha deveres de diligência e lealdade

cujo descumprimento pode gerar responsabilidade pessoal. A LGPD, embora focada em pessoas jurídicas, não exclui responsabilização de pessoas físicas em contextos específicos.

O dever de diligência dos administradores inclui, na interpretação contemporânea, a supervisão adequada de riscos cibernéticos. Assim como administradores não podem alegar desconhecimento de riscos financeiros ou operacionais evidentes, tampouco podem ignorar riscos digitais que afetam a continuidade e a reputação da organização. A Securities and Exchange Commission (SEC, comissão de valores mobiliários norte-americana) tem progressivamente responsabilizado executivos por falhas de disclosure (divulgação obrigatória) relacionadas a incidentes cibernéticos. A tendência é global e alcançará o Brasil com defasagem cada vez menor.

A distinção entre risco assumido conscientemente e risco ignorado negligentemente é determinante. Um conselho de administração que analisa relatórios de segurança, questiona a gestão, aprova investimentos proporcionais e monitora implementação demonstra supervisão ativa, ainda que um incidente eventualmente ocorra. Um conselho que jamais pautou o tema, não recebe relatórios e desconhece a postura de segurança da organização demonstra omissão que pode configurar violação do dever de diligência.

Os CIS Controls oferecem aos administradores ferramenta para exercer supervisão informada mesmo sem expertise técnica. As métricas de implementação são compreensíveis: quantos por cento dos ativos estão inventariados? Qual o tempo médio para correção de vulnerabilidades críticas? Quantos colaboradores completaram treinamento de segurança? Essas perguntas não exigem formação técnica para serem formuladas ou compreendidas. Administradores que as formulam regularmente demonstram engajamento; aqueles que não as formulam demonstram desinteresse.

A documentação de deliberações sobre segurança cibernética em atas de conselho e comitês constitui evidência crucial. Registrar que o tema foi discutido, que relatórios foram analisados, que investimentos foram aprovados, que riscos residuais foram conscientemente aceitos. Esse acervo protege administradores contra alegações de omissão. A ausência de qualquer registro sugere que o tema simplesmente não existia na agenda da governança, configurando negligência institucionalizada.

O caso SolarWinds (2020) estabeleceu precedente significativo nessa matéria. A SEC processou a empresa e seu Chief Information Security Officer (CISO, diretor executivo de segurança da informação) por alegadas declarações enganosas sobre práticas de segurança que não correspondiam à realidade operacional. A mensagem para o mercado foi clara: executivos de segurança respondem pessoalmente pela veracidade das informações que divulgam sobre a postura de segurança da organização.

3.7 Casos de Referência: Ausência de Controles Básicos e Suas Consequências

A análise de casos concretos ilumina como a ausência de controles fundamentais, precisamente aqueles endereçados pelos CIS Controls, agrava consequências jurídicas e regulatórias de incidentes.

Equifax (2017): O vazamento de dados de aproximadamente 147 milhões de consumidores norte-americanos originou-se de vulnerabilidade conhecida no Apache Struts, para a qual correção estava disponível havia meses. A Federal Trade Commission e múltiplos reguladores estaduais identificaram falhas elementares: a empresa não mantinha inventário adequado de sistemas (Controle 1), não implementava processo efetivo de gestão de vulnerabilidades (Controle 7), não segmentava adequadamente sua rede (Controle 12). O acordo final superou 700 milhões de dólares, incluindo fundo de compensação a consumidores e investimentos obrigatórios em segurança. (Fonte: ftc.gov/enforcement/cases-proceedings/refunds/equifax-data-breach-settlement)

British Airways (2018): O Information Commissioner's Office britânico aplicou multa de 20 milhões de libras após vazamento de dados de aproximadamente 400 mil clientes. A investigação identificou que atacantes acessaram sistemas através de credenciais comprometidas de fornecedor terceirizado, falha endereçada pelo Controle 5 (Gestão de Contas) e Controle 15 (Gestão de Provedores de Serviços). A ausência de autenticação multifator para acessos privilegiados e monitoramento inadequado de atividades anômalas agravaram a avaliação regulatória. O ICO explicitamente considerou que medidas de segurança "não eram adequadas ao risco." (Fonte: ico.org.uk/action-weve-taken/enforcement/british-airways/)

Marriott International (2020): Multa de 18,4 milhões de libras pelo ICO após vazamento de dados de aproximadamente 339 milhões de hóspedes. A investigação revelou que a empresa não realizou due diligence (diligência prévia) adequada de segurança quando adquiriu a rede Starwood, herdando sistemas comprometidos que permaneceram não detectados por anos. A falha mapeia diretamente para o Controle 1 (conhecer o que se possui) e o Controle 8 (manter logs que permitam detecção). O caso demonstra que responsabilidade por segurança cibernética inclui diligência em fusões e aquisições.

Contexto Brasileiro: A Atuação da ANPD

A realidade brasileira oferece lições específicas que merecem atenção de PMEs, consultores e advogados que atuam no mercado nacional. A ANPD, embora ainda construindo jurisprudência, já aplicou sanções que evidenciam expectativas alinhadas aos CIS Controls.

Telekall Infoservice (julho de 2023): A primeira sanção pecuniária da ANPD foi aplicada a uma microempresa de telecomunicações que comercializava listas de contatos de WhatsApp de eleitores para campanhas políticas. A multa totalizou R$ 14.400,00, correspondendo ao teto legal de 2% do faturamento bruto para o porte da empresa. As infrações identificadas incluíram tratamento de dados sem base legal (Art. 7º da LGPD), ausência de encarregado de proteção de dados (Art. 41) e não atendimento às determinações da fiscalização. A mensagem foi inequívoca: o porte reduzido da empresa não constitui escudo contra fiscalização. (Fonte: gov.br/anpd/pt-br/assuntos/noticias/anpd-aplica-a-primeira-multa-por-descumprimento-a-lgpd)

Instituto Nacional do Seguro Social, INSS (fevereiro de 2024): Sanção de publicização aplicada pela ausência de comunicação aos titulares sobre incidente de segurança ocorrido em 2022. O incidente afetou o Sistema Corporativo de Benefícios (SISBEN), expondo informações como CPF, dados bancários e data de nascimento. Foram identificadas mais de 90 milhões de consultas ao SISBEN e 9 milhões ao Sistema Único de Benefícios (DATAPREV) realizadas sem justificativa operacional. O INSS alegou inviabilidade técnica para individualizar as pessoas afetadas, mas a ANPD rejeitou a justificativa, apontando que a comunicação poderia ter sido realizada de forma indireta através de ampla divulgação. A condenação determinou publicação de comunicado no site principal e no aplicativo "Meu INSS" por 60 dias. (Fonte: gov.br/anpd/pt-br/assuntos/noticias/anpd-sanciona-inss-e-secretaria-de-educacao-do-df-por-violacoes-a-lgpd)

Instituto de Assistência ao Servidor Público Estadual de São Paulo, IAMSPE (outubro de 2023): Advertência aplicada por comunicação insuficiente de incidente de segurança. Embora a entidade tenha publicado comunicado em seu site, o conteúdo foi considerado inadequado pela ANPD. O caso revelou ainda ausência de manutenção de logs, tornando impossível identificar quais dados foram efetivamente comprometidos e quais titulares foram afetados. A lição é direta: sem registros de auditoria adequados (Controle 8 dos CIS Controls), a organização não consegue sequer mensurar a extensão do dano.

Secretaria de Estado de Educação do Distrito Federal, SEEDF (janeiro de 2024): Quatro sanções de advertência aplicadas por múltiplas infrações: ausência de registro de operações de tratamento de dados pessoais (Art. 37), não elaboração de Relatório de Impacto à Proteção de Dados Pessoais após solicitação da ANPD (Art. 38), ausência de comunicação de incidente aos titulares (Art. 48) e uso de sistemas que não atendiam requisitos de segurança (Art. 5º do Regulamento de Fiscalização). O caso ilustra como a negligência em documentação e procedimentos básicos multiplica as infrações identificadas em um único processo.

Secretaria de Estado da Saúde de Santa Catarina (2024): Sancionada por ausência de comunicação a titulares sobre incidente de segurança, ausência de medidas de segurança adequadas e não atendimento a determinações da ANPD. O processo evidenciou fragilidades sistêmicas na proteção de dados sensíveis de saúde.

Secretaria de Assistência Social, Combate à Fome e Políticas sobre Drogas de Pernambuco (2024): Sancionada após incidente que expôs dados de populações vulneráveis atendidas por programas sociais. O caso demonstra a sensibilidade particular de dados tratados por órgãos de assistência social.

Panorama Quantitativo: A Escalada dos Incidentes no Brasil em 2025

Os números de 2025 contextualizam a urgência da adoção de controles estruturados com clareza inquestionável. O Brasil consolidou posição como um dos principais alvos globais de ataques cibernéticos, com indicadores que superaram significativamente os anos anteriores.

O relatório do FortiGuard Labs, apresentado no Fortinet Cybersecurity Summit Brasil 2025 em agosto, revelou que o Brasil registrou 315 bilhões de tentativas de ataques cibernéticos apenas no primeiro semestre de 2025. Esse volume representa 84% de todas as tentativas detectadas na América Latina no período, que totalizou 374 bilhões. Para dimensionar: são aproximadamente 1.379 tentativas de ataque por minuto contra organizações brasileiras. México ficou em distante segundo lugar, com 10,8% do total regional, seguido por Colômbia (1,89%) e Chile (0,1%). A metodologia Cyber Kill Chain (cadeia de ataque cibernético) utilizada no relatório identificou, na fase de ação final, 309 bilhões de tentativas de negação de serviço (DDoS) e 28,1 mil incidentes de ransomware (sequestro de dados mediante extorsão) no país.

O custo financeiro dessas violações também escalou. O relatório Cost of a Data Breach 2025, publicado pela IBM em julho, revelou que o custo médio de uma violação de dados no Brasil atingiu R$ 7,19 milhões, aumento de 6,5% em relação aos R$ 6,75 milhões de 2024. Os setores mais impactados foram Saúde (R$ 11,43 milhões por incidente), Finanças (R$ 8,92 milhões) e Serviços (R$ 8,51 milhões). O phishing (golpe de engenharia social por e-mail ou mensagem) emergiu como principal vetor de ataque, responsável por 18% das violações, seguido por comprometimento de terceiros e cadeia de suprimentos (15%) e exploração de vulnerabilidades (13%).

A pesquisa global de vazamentos de dados da Surfshark registrou que o Brasil acumulou aproximadamente 1,3 milhão de contas violadas no primeiro semestre de 2025 (702,2 mil no primeiro trimestre e 639,6 mil no segundo), posicionando o país entre os dez mais afetados mundialmente. Estatisticamente, cada brasileiro conectado foi afetado aproximadamente duas vezes por violações de dados desde 2004, quando a série histórica teve início. O país acumula 417 milhões de contas de usuário comprometidas nesse período, com 170,3 milhões de senhas vazadas junto às credenciais.

Incidentes específicos de 2025 ilustram a materialização desses riscos. Em março, o Banco Central comunicou o primeiro vazamento de chaves Pix do ano, envolvendo 25.349 registros vinculados à fintech QI Sociedade de Crédito Direto S.A. Os dados expostos, embora limitados a informações cadastrais (nome, CPF com

máscara, agência, número e tipo de conta), não incluíram senhas ou saldos. A vulnerabilidade ocorreu entre 23 de fevereiro e 6 de março, decorrente de falhas pontuais nos sistemas da instituição.

Em junho de 2025, pesquisadores do portal Cybernews revelaram o que classificaram como o maior vazamento de credenciais já registrado: mais de 16 bilhões de logins e senhas de plataformas como Google, Apple, Facebook, Telegram, GitHub e serviços governamentais. Os dados foram compilados a partir de 30 bases distintas, muitas contendo informações nunca antes identificadas em vazamentos públicos. Mais de 3,5 bilhões de registros foram associados a usuários de língua portuguesa, indicando impacto significativo sobre o Brasil. As credenciais, organizadas em formato URL/login/senha, foram obtidas predominantemente por malwares do tipo infostealer (programas espiões que capturam credenciais diretamente dos dispositivos infectados).

A discrepância entre a atuação fiscalizatória da ANPD e reguladores internacionais permanece, mas mostra sinais de mudança. Em 2024, segundo levantamento do escritório L.O. Baptista Advogados, enquanto União Europeia, Reino Unido, Estados Unidos, Argentina e Austrália aplicaram, somados, US$ 1,7 bilhão em multas por infrações relacionadas à proteção de dados, o Brasil não aplicou nenhuma multa pecuniária no mesmo período. A Agenda Regulatória da ANPD para 2025-2026, contudo, sinaliza fortalecimento da função fiscalizatória, e especialistas projetam intensificação das ações sancionadoras nos próximos anos.

Para PMEs, consultores e advogados, o cenário exige atenção redobrada. As organizações já sancionadas pela ANPD apresentavam lacunas elementares que os CIS Controls endereçam diretamente: ausência de encarregado de dados, falta de comunicação de incidentes, inexistência de registros de operações, sistemas sem requisitos mínimos de segurança. O padrão é consistente e previsível. Implementar controles básicos não é mais diferencial competitivo; tornou-se condição de sobrevivência em ambiente regulatório e de ameaças que amadurece rapidamente.

A Associação Nacional dos Profissionais de Privacidade de Dados (APDADOS) mantém repositório público de violações e sanções relacionadas à proteção de dados no Brasil, disponível em apdados.org/violacoes[7], recurso valioso para acompanhamento da evolução do enforcement (aplicação de sanções) nacional.

[7] Violações LGPD – APDADOS – Disponível em: https://apdados.org/violacoes - Acesso jan. 2026
Avalie a data de entrada das reclamações e as datas de multas pagas.

Referências do Capítulo

ASSOCIAÇÃO NACIONAL DOS PROFISSIONAIS DE PRIVACIDADE DE DADOS. Repositório de Violações. São Paulo: APDADOS, 2025. Disponível em: https://apdados.org/violacoes. Acesso em: 16 jan. 2026.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. ANPD aplica a primeira multa por descumprimento à LGPD. Brasília: ANPD, 2023. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-aplica-a-primeira-multa-por-descumprimento-a-lgpd. Acesso em: 16 jan. 2026.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. ANPD sanciona INSS e Secretaria de Educação do DF por violações à LGPD. Brasília: ANPD, 2024. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-sanciona-inss-e-secretaria-de-educacao-do-df-por-violacoes-a-lgpd. Acesso em: 16 jan. 2026.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Decisões em processos sancionadores. Brasília: ANPD, 2025. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/decisoes-em-processos-sancionadores-1. Acesso em: 16 jan. 2026.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Guia Orientativo sobre Segurança da Informação para Agentes de Tratamento de Pequeno Porte. Brasília: ANPD, 2021. Disponível em: https://www.gov.br/anpd/pt-br. Acesso em: 16 jan. 2026.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Resolução CD/ANPD nº 15, de 2024. Regulamento de Comunicação de Incidentes de Segurança. Brasília: ANPD, 2024.

BANCO CENTRAL DO BRASIL. Comunicado de vazamento de dados cadastrais vinculados a chaves Pix. Brasília: BCB, 2025. Disponível em: https://www.bcb.gov.br. Acesso em: 16 jan. 2026.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 16 jan. 2026.

CENTER FOR INTERNET SECURITY. CIS Controls v8.1. East Greenbush: CIS, 2024. Disponível em: https://www.cisecurity.org/controls. Acesso em: 16 jan. 2026.

CYBERNEWS. 16 Billion Credentials Exposed in Largest Data Breach Ever Recorded. Vilnius: Cybernews, 2025. Disponível em: https://cybernews.com. Acesso em: 16 jan. 2026.

FEDERAL TRADE COMMISSION. Equifax Data Breach Settlement. Washington: FTC, 2019. Disponível em: https://www.ftc.gov/enforcement/cases-proceedings/refunds/equifax-data-breach-settlement. Acesso em: 16 jan. 2026.

FORTIGUARD LABS. Cenário Global de Ameaças: América Latina 1º Semestre 2025. Sunnyvale: Fortinet, 2025. Disponível em: https://www.fortinet.com/br. Acesso em: 16 jan. 2026.

IBM SECURITY. Cost of a Data Breach Report 2025. Armonk: IBM, 2025. Disponível em: https://brasil.newsroom.ibm.com/2025-07-30-Relatorio-da-IBM-Custo-medio-de-uma-violacao-de-dados-no-Brasil-atinge-R-7,19-milhoes. Acesso em: 16 jan. 2026.

INFORMATION COMMISSIONER'S OFFICE. Penalty Notice: British Airways. Londres: ICO, 2020. Disponível em: https://ico.org.uk/action-weve-taken/enforcement/british-airways/. Acesso em: 16 jan. 2026.

L.O. BAPTISTA ADVOGADOS. Levantamento de Multas Globais por Proteção de Dados 2024. São Paulo: L.O. Baptista, 2025. Disponível em: https://www.baptista.com.br/anpd-nao-multou-empresas-por-violacao-da-lgpd-em-2024/ - https://valor.globo.com/legislacao/noticia/2025/01/29/anpd-nao-multou-empresas-por-violacao-da-lgpd-em-2024.ghtml - Acesso jan. 2026

SECURITIES AND EXCHANGE COMMISSION. SEC Charges SolarWinds and Chief Information Security Officer with Fraud, Internal Control Failures. Washington: SEC, 2023. Disponível em: https://www.sec.gov/litigation. Acesso em: 16 jan. 2026.

SURFSHARK. Global Data Breach Monitoring: Brazil Q1-Q2 2025. Vilnius: Surfshark, 2025. Disponível em: https://surfshark.com/research/data-breach-monitoring?country=br. Acesso em: 16 jan. 2026.

CAPÍTULO 4 - CIS e Priorização em Ambientes com Poucos Recursos

4.1 Por que "Fazer Tudo" é Impossível, Fazer Nada não é desculpa

A objeção mais frequente que executivos de pequenas e médias empresas levantam quando confrontados com frameworks de segurança é previsível: "não temos recursos para implementar tudo isso." A afirmação é verdadeira. Nenhuma organização, independentemente de porte ou orçamento, consegue implementar simultaneamente todos os controles de todos os frameworks disponíveis. Essa impossibilidade, entretanto, não justifica a inação. Justifica priorização.

O erro conceitual reside na premissa binária de que segurança seria escolha entre "fazer tudo" ou "não fazer nada." Essa falsa dicotomia paralisa organizações que poderiam, com investimento modesto, eliminar a maior parte de sua exposição a ataques comuns. A realidade operacional de incidentes cibernéticos revela padrão consistente: a maioria esmagadora das violações bem-sucedidas explora vulnerabilidades elementares, não sofisticação técnica extraordinária. Credenciais fracas ou reutilizadas. Sistemas desatualizados com vulnerabilidades conhecidas. Ausência de inventário que permita saber o que proteger. Falta de backup que transforme ransomware (sequestro de dados mediante extorsão) em catástrofe.

Atacantes seguem a lógica do menor esforço. Por que desenvolver exploits (códigos de exploração) sofisticados contra defesas robustas quando milhares de organizações deixam portas abertas?

O relatório Global Threat Landscape 2025 da Fortinet[8] indica que, no primeiro semestre de 2025, o Brasil sofreu cerca de 315 bilhões de tentativas de ataques cibernéticos, representando 84% das tentativas na América Latina. O mesmo relatório destaca, em seu panorama global, que uma parcela substancial dessas tentativas explora vulnerabilidades já conhecidas, com correções disponíveis, evidenciando que o principal problema não é a falta de solução técnica, mas a falta de aplicação consistente de controles básicos, como gestão de patches e de configuração segura.

O CIS Controls foi desenhado precisamente para endereçar essa realidade. Não parte da premissa de recursos infinitos ou ambientes ideais. Parte da premissa de que organizações reais operam com orçamentos limitados, equipes reduzidas e prioridades concorrentes. A estrutura de Implementation Groups (grupos de implementação graduados por maturidade) reconhece explicitamente que diferentes organizações têm diferentes capacidades e diferentes perfis de risco. O que o framework não aceita é a alegação de que nada pode ser feito.

[8] EXAME. Brasil registra 315 bilhões de tentativas de ataques cibernéticos somente em 2025, aponta Fortinet. 2025. Disponível em: https://exame.com/inteligencia-artificial/brasil-registra-315-bilhoes-de-tentativas-de-ataques-ciberneticos-somente-em-2025-aponta-fortinet/ - Acesso em: jan. 2026.

A pergunta relevante não é "podemos implementar todos os controles?" A pergunta relevante é: "dado nosso contexto, quais controles eliminam a maior parte do risco com o menor investimento?" Essa é a lógica de priorização que transforma frameworks extensos em programas viáveis.

4.2 Implementation Group 1: O Baseline Universal

O Center for Internet Security organizou os CIS Controls em três Implementation Groups (IGs) que representam níveis progressivos de maturidade e capacidade. Essa estrutura não é arbitrária; reflete análise sistemática de quais controles oferecem maior retorno de proteção para diferentes perfis organizacionais.

O Implementation Group 1 (IG1) constitui o que o CIS denomina "cyber hygiene" (higiene cibernética) essencial, o conjunto mínimo de salvaguardas que qualquer organização, independentemente de porte ou setor, deveria implementar. O IG1 foi desenhado especificamente para organizações com recursos limitados de TI e segurança, onde a equipe técnica pode ser pequena ou mesmo inexistente como função dedicada. A premissa é direta: se uma organização não consegue implementar nem mesmo o IG1, está operando abaixo do limiar mínimo de diligência razoável.

O IG1 compreende 56 salvaguardas distribuídas pelos 18 controles do framework. Esse número pode parecer elevado à primeira vista, mas é necessário contextualizar. Muitas dessas salvaguardas são simples configurações que podem ser implementadas em horas, não em meses. Outras são práticas que organizações minimamente estruturadas já deveriam estar executando por razões operacionais básicas, não apenas de segurança. O IG1 não exige tecnologias caras ou especialistas dedicados. Exige decisão, disciplina e documentação.

A lógica de seleção das salvaguardas do IG1 seguiu critérios específicos: eficácia comprovada contra ataques comuns, viabilidade de implementação com recursos limitados e independência de tecnologias proprietárias específicas. O resultado é um conjunto que, quando implementado integralmente, protege a organização contra a maioria dos ataques oportunistas que constituem o grosso das ameaças enfrentadas por PMEs.

O Implementation Group 2 (IG2) adiciona salvaguardas para organizações que tratam dados sensíveis, operam infraestrutura crítica ou enfrentam adversários mais sofisticados. Pressupõe equipe de TI com alguma especialização em segurança e capacidade de implementar controles mais complexos. O Implementation Group 3 (IG3) contempla organizações que enfrentam adversários avançados, incluindo atores estatais, e requer capacidades especializadas de defesa e resposta.

Para a maioria das PMEs brasileiras, o IG1 representa não apenas o ponto de partida, mas potencialmente o programa completo de segurança adequado ao seu perfil de risco. Organizações que implementam integralmente o IG1 já se posicionam significativamente acima da média do mercado em termos de postura defensiva.

4.3 Os 56 Safeguards do IG1: O Mínimo Defensável

Examinar as 56 salvaguardas do IG1 revela que o "mínimo defensável" é simultaneamente mais acessível e mais abrangente do que muitos executivos imaginam. O framework distribui essas salvaguardas pelos 18 controles, criando cobertura que endereça as principais superfícies de ataque.

Inventário e Gestão de Ativos (Controles 1 e 2): O IG1 inclui salvaguardas para estabelecer e manter inventário de ativos corporativos (hardware) e de software. A lógica é elementar: não é possível proteger o que não se conhece. Organizações que não sabem quantos dispositivos estão conectados à sua rede, quais softwares estão instalados ou quais serviços em nuvem seus colaboradores utilizam operam no escuro. As salvaguardas do IG1 não exigem ferramentas sofisticadas de descoberta automática; podem ser implementadas inicialmente com planilhas estruturadas e processos de atualização periódica.

Proteção de Dados (Controle 3): Salvaguardas para estabelecer processos de gestão de dados, incluindo identificação de dados sensíveis, configuração de controles de acesso e práticas de descarte seguro. O IG1 não exige implementação de DLP (Data Loss Prevention, prevenção de perda de dados) sofisticado, mas demanda consciência sobre onde dados sensíveis residem e quem pode acessá-los.

Configuração Segura (Controle 4): Processos para estabelecer e manter configurações seguras de ativos corporativos e software. Inclui remoção de configurações padrão inseguras, desabilitação de serviços desnecessários e aplicação de hardening (fortalecimento de configuração) básico. Muitas violações exploram configurações de fábrica que nunca foram alteradas.

Gestão de Contas (Controle 5): Salvaguardas para gerenciar credenciais e contas de usuários. Inclui inventário de contas, processos de concessão e revogação de acesso, políticas de senhas e desabilitação de contas padrão. O IG1 também inclui implementação de MFA (Multi-Factor Authentication, autenticação multifator) para aplicações expostas externamente, reconhecendo que senhas sozinhas são proteção insuficiente.

Gestão de Controle de Acesso (Controle 6): Processos para criar, atribuir, gerenciar e revogar credenciais e privilégios de acesso. Implementação do princípio de menor privilégio, onde usuários recebem apenas os acessos necessários para suas funções.

Gestão Contínua de Vulnerabilidades (Controle 7): Processos para identificar, priorizar e remediar vulnerabilidades. O IG1 não exige scanners (ferramentas de varredura) comerciais sofisticados, mas demanda processo estabelecido para aplicação de patches (correções de segurança) e atualizações de segurança. A janela entre divulgação de vulnerabilidade e aplicação de correção é frequentemente o período em que ataques ocorrem.

Gestão de Registros de Auditoria (Controle 8): Salvaguardas para coletar, alertar, revisar e reter logs (registros de eventos) de auditoria. Sem registros, não há como detectar incidentes, investigar violações ou demonstrar diligência. O IG1 exige que logs existam e sejam retidos por período adequado, não que sejam analisados em tempo real por SIEM (Security Information and Event Management, sistema de gerenciamento de informações e eventos de segurança) sofisticado.

Proteções de E-mail e Navegador Web (Controle 9): Configurações de segurança para clientes de e-mail e navegadores, incluindo proteção contra phishing (golpe de engenharia social) e downloads maliciosos. Considerando que e-mail permanece o vetor de ataque mais comum, essas salvaguardas oferecem retorno significativo.

Defesas Contra Malware (Controle 10): Implementação de software anti-malware e configurações que previnam execução de código malicioso. O IG1 não exige soluções EDR (Endpoint Detection and Response, detecção e resposta em endpoint) avançadas, mas demanda proteção básica contra ameaças conhecidas.

Recuperação de Dados (Controle 11): Salvaguardas para backup e recuperação de dados. Inclui realização de backups regulares, armazenamento seguro (preferencialmente offline ou em local separado) e testes periódicos de restauração. Organizações com backup funcional e testado transformam ransomware de catástrofe em inconveniência.

Gestão de Infraestrutura de Rede (Controle 12): Configurações seguras de dispositivos de rede. O IG1 inclui salvaguardas básicas como alteração de credenciais padrão em roteadores e switches, segmentação básica de rede e configuração de firewall (barreira de proteção de rede).

Monitoramento e Defesa de Rede (Controle 13): Salvaguardas para monitorar e defender a infraestrutura de rede. O IG1 foca em capacidades básicas de detecção, não em SOC (Security Operations Center, centro de operações de segurança) 24/7.

Conscientização e Treinamento em Segurança (Controle 14): Programa de conscientização para colaboradores. Inclui treinamento sobre reconhecimento de phishing, práticas seguras de senhas e procedimentos de reporte de incidentes. O fator humano permanece vetor crítico de ataque; investimento em conscientização oferece retorno desproporcional ao custo.

Gestão de Provedores de Serviços (Controle 15): Processos para avaliar e gerenciar provedores que tratam dados sensíveis ou operam infraestrutura crítica. Inclui inventário de provedores, avaliação de práticas de segurança e cláusulas contratuais adequadas.

Segurança de Software de Aplicação (Controle 16): Salvaguardas para desenvolvimento e aquisição segura de software. O IG1 inclui salvaguardas básicas aplicáveis mesmo a organizações que não desenvolvem software internamente, como verificação de integridade de software adquirido.

Gestão de Resposta a Incidentes (Controle 17): Processos para detectar, responder e recuperar de incidentes. O IG1 exige que a organização tenha plano documentado, equipe designada e procedimentos básicos de comunicação. Não exige capacidade de resposta 24/7 ou equipe dedicada de incident response (resposta a incidentes).

Testes de Penetração (Controle 18): O IG1 não inclui salvaguardas deste controle, reconhecendo que testes de penetração requerem capacidades que excedem o perfil de organizações em nível básico de maturidade.

A soma dessas salvaguardas constitui programa de segurança completo para organizações de menor porte. Implementá-las integralmente posiciona a organização acima da maioria de seus pares em termos de postura defensiva.

4.4 O CIS como Filtro do que Realmente Importa

A proliferação de frameworks, normas, regulamentos e recomendações de segurança cria paradoxo para gestores: quanto mais informação disponível, mais difícil decidir por onde começar. O CIS Controls, especialmente através da estrutura de Implementation Groups, funciona como filtro que separa o essencial do desejável.

O critério de seleção das salvaguardas do IG1 seguiu metodologia específica: cada salvaguarda foi avaliada quanto à sua eficácia contra ataques documentados, quanto à viabilidade de implementação em ambientes com recursos limitados e quanto à independência de tecnologias específicas. O resultado é lista curada que representa o consenso de especialistas sobre o que realmente importa no nível básico.

Esse filtro resolve problema comum em organizações menores: a paralisia por excesso de opções. Quando um empresário ou gestor de TI pesquisa "como melhorar segurança da empresa," encontra dezenas de recomendações, produtos e serviços concorrentes. Sem critério de priorização, a tendência é ou implementar aleatoriamente o que parecer mais acessível, ou não implementar nada por incapacidade de decidir.

O IG1 oferece resposta objetiva: estas são as 56 salvaguardas que você precisa implementar primeiro. Não porque são as únicas importantes, mas porque são as que oferecem maior proteção com menor investimento. Quando estiverem implementadas, avalie se seu perfil de risco justifica avançar para IG2. Essa clareza de priorização é particularmente valiosa para organizações sem especialistas internos de segurança.

A estrutura também facilita comunicação com partes externas. Quando um auditor pergunta "como está a segurança da organização?" ou quando uma seguradora solicita informações para subscrição de apólice cyber, a resposta "implementamos integralmente o IG1 do CIS Controls" é compreensível e verificável.

Comunicação baseada em framework reconhecido substitui alegações vagas por demonstração objetiva.

4.5 O Custo Invisível de Não Priorizar

A decisão de postergar implementação de controles básicos frequentemente se baseia em cálculo de custo imediato: quanto custa implementar versus quanto custa não implementar agora. Esse cálculo tipicamente subestima o custo da inação porque considera apenas despesas diretas visíveis, ignorando custos que permanecem ocultos até se materializarem.

O custo médio de uma violação de dados no Brasil atingiu R$ 7,19 milhões em 2025, segundo o relatório Cost of a Data Breach da IBM. Para PMEs, mesmo incidentes menores podem representar valores que excedem significativamente o que seria necessário para implementar o IG1 completo. Um único ataque de ransomware bem-sucedido pode gerar custos diretos (resgate, se pago; recuperação de sistemas; horas de trabalho perdidas) e indiretos (danos reputacionais, perda de clientes, aumento de prêmios de seguro) que ultrapassam anos de investimento em segurança básica.

Os custos invisíveis da não priorização incluem:

Seguros negados ou encarecidos: Seguradoras de risco cyber avaliam controles implementados antes de subscrever apólices. Organizações sem controles básicos enfrentam prêmios significativamente mais altos ou recusa de cobertura. Pior: em caso de sinistro, a ausência de controles pode ser invocada como violação de garantias contratuais, comprometendo a cobertura.

Litígios perdidos: Conforme demonstrado no Capítulo 3, a ausência de controles básicos agrava responsabilização em litígios decorrentes de incidentes. O que poderia ser tratado como risco inerente à atividade (incidente apesar de diligência) transforma-se em negligência (incidente por ausência de diligência).

Sanções regulatórias agravadas: A ANPD, ao avaliar sanções, considera se a organização mantinha medidas de segurança adequadas. Organizações que demonstram programa estruturado de segurança, mesmo que o incidente tenha ocorrido, posicionam-se melhor do que aquelas que não tinham qualquer estrutura.

Oportunidades de negócio perdidas: Crescentemente, grandes empresas e órgãos públicos exigem demonstração de práticas de segurança de seus fornecedores. PMEs que não conseguem demonstrar controles básicos são excluídas de processos de contratação ou têm contratos rescindidos.

Tempo de recuperação estendido: Organizações sem backup testado, sem plano de resposta a incidentes e sem documentação de seus sistemas levam semanas ou

meses para recuperar operações após incidentes. Organizações preparadas recuperam em dias ou horas.

O cálculo correto de custo-benefício compara o investimento em controles básicos não com zero, mas com a expectativa matemática de perdas caso um incidente ocorra, ponderada pela probabilidade de ocorrência. Dado o volume de ataques documentado (315 bilhões de tentativas contra organizações brasileiras apenas no primeiro semestre de 2025), a probabilidade de ser alvo deixou de ser questão de "se" para tornar-se questão de "quando."

4.6 Como PMEs Podem Usar o IG1 como Programa Completo de Segurança

Para pequenas e médias empresas, o IG1 pode constituir não apenas ponto de partida, mas programa completo de segurança adequado ao seu perfil de risco. Essa afirmação não representa concessão ou redução de padrão; reflete a realidade de que diferentes organizações enfrentam diferentes ameaças e possuem diferentes capacidades.

Uma PME que implementa integralmente o IG1 está protegida contra a maioria dos ataques oportunistas que constituem o grosso das ameaças enfrentadas por organizações de seu porte. Atacantes sofisticados com recursos significativos tipicamente direcionam esforços contra alvos de alto valor (instituições financeiras, infraestrutura crítica, grandes corporações com dados valiosos), não contra empresas menores cujos dados têm valor limitado no mercado criminoso.

Isso não significa que PMEs nunca são atacadas por adversários sofisticados, ou que o IG1 as torna imunes a qualquer ameaça. Significa que, dado o perfil de risco típico de uma PME, o IG1 oferece proteção proporcional. Organizações que tratam dados particularmente sensíveis (saúde, financeiro), que fazem parte de cadeias de suprimentos críticas ou que por qualquer razão possam atrair atenção de adversários mais sofisticados devem avaliar se IG2 ou IG3 são mais apropriados para seu contexto.

A implementação do IG1 como programa completo demanda abordagem estruturada:

Fase 1: Inventário e Visibilidade (Controles 1, 2, 3). Estabelecer conhecimento sobre o que a organização possui: quais dispositivos, quais softwares, quais dados, onde estão localizados. Sem essa fundação, controles subsequentes não podem ser efetivamente implementados.

Fase 2: Proteção de Acesso (Controles 4, 5, 6). Configurar sistemas de forma segura, estabelecer gestão de contas e implementar controles de acesso. Inclui implementação de MFA para sistemas críticos e externos.

Fase 3: Defesa e Detecção (Controles 7, 8, 9, 10, 12, 13). Implementar gestão de vulnerabilidades, logging (registro de eventos), proteções de e-mail e navegador, defesas contra malware e configuração segura de rede.

Fase 4: Resiliência (Controles 11, 17). Estabelecer processos de backup e recuperação, e desenvolver capacidade básica de resposta a incidentes.

Fase 5: Fator Humano e Terceiros (Controles 14, 15, 16). Implementar programa de conscientização, estabelecer gestão de provedores e garantir práticas básicas de segurança de software.

Essa sequência não é rígida, mas reflete dependências lógicas: não faz sentido implementar controles de acesso sofisticados sem saber quais sistemas existem, nem desenvolver plano de resposta a incidentes sem capacidade de detectar que um incidente ocorreu.

O tempo necessário para implementação completa do IG1 varia conforme o estado inicial da organização, mas uma PME típica pode alcançar implementação substancial em três a seis meses com dedicação de recursos limitados. Organizações que partem de maturidade zero podem precisar de período mais extenso; organizações que já possuem práticas informais de segurança podem formalizar e complementar mais rapidamente.

4.7 Progressão para IG2 e IG3: Quando e Por que Evoluir

A estrutura de Implementation Groups não implica que todas as organizações devam eventualmente progredir para IG3. Implica que diferentes organizações têm diferentes níveis apropriados de controles, e que esses níveis podem mudar conforme o contexto organizacional evolui.

A decisão de progredir do IG1 para IG2 deve considerar fatores específicos:

Mudança no perfil de dados tratados: Se a organização passa a tratar dados sensíveis que anteriormente não tratava (dados de saúde, dados financeiros detalhados, dados de menores), o perfil de risco muda e controles adicionais podem ser necessários.

Inclusão em cadeia de suprimentos crítica: Se a organização torna-se fornecedor de empresa maior que exige níveis mais elevados de segurança, ou se passa a participar de infraestrutura crítica (energia, telecomunicações, financeiro), controles adicionais são justificados.

Evidência de targeting (direcionamento) específico: Se a organização identifica que está sendo especificamente visada por adversários (não apenas alvos de ataques oportunistas), o perfil de ameaça mudou e defesas mais robustas são necessárias.

Crescimento que aumenta atratividade como alvo: Organizações que crescem significativamente em faturamento, em volume de dados tratados ou em relevância de mercado podem tornar-se alvos mais atrativos, justificando controles adicionais.

Exigências regulatórias específicas: Setores regulados podem ter exigências que excedem o IG1, demandando implementação de controles de nível superior para conformidade.

O IG2 adiciona 74 salvaguardas às 56 do IG1, totalizando 130. Essas salvaguardas adicionais presumem equipe de TI com alguma especialização em segurança e capacidade de implementar e manter controles mais complexos. Incluem, por exemplo, monitoramento mais sofisticado, segmentação de rede mais granular e capacidades mais robustas de detecção e resposta.

O IG3 adiciona 23 salvaguardas às 130 do IG2, totalizando 153 (o conjunto completo do framework). Essas salvaguardas são desenhadas para organizações que enfrentam adversários sofisticados, incluindo potencialmente atores estatais. Presumem capacidades avançadas de segurança, frequentemente incluindo equipe dedicada e tecnologias especializadas.

A progressão não precisa ser linear ou completa. Uma organização pode implementar o IG1 integralmente, avaliar que apenas algumas salvaguardas específicas do IG2 são relevantes para seu contexto e implementá-las seletivamente. O framework oferece estrutura, não camisa de força.

O critério orientador permanece proporcionalidade: os controles implementados devem ser proporcionais aos riscos enfrentados e às capacidades da organização. Implementar controles de IG3 em PME com perfil de risco baixo representa desperdício de recursos que poderiam ser melhor aplicados. Manter apenas IG1 em organização que trata dados altamente sensíveis e enfrenta adversários sofisticados representa exposição inaceitável. O julgamento sobre o nível apropriado é responsabilidade da governança, informada por avaliação de risco e aconselhamento técnico.

Referências do Capítulo

CENTER FOR INTERNET SECURITY. CIS Controls v8.1. East Greenbush: CIS, 2024. Disponível em: https://www.cisecurity.org/controls. Acesso em: 16 jan. 2026.

CENTER FOR INTERNET SECURITY. CIS Controls v8.1 Implementation Guide for Small and Medium Enterprises. East Greenbush: CIS, 2024. Disponível em: https://www.cisecurity.org/controls/implementation-groups. Acesso em: 16 jan. 2026.

FORTIGUARD LABS. Cenário Global de Ameaças: América Latina 1º Semestre 2025. Sunnyvale: Fortinet, 2025. Disponível em: https://www.fortinet.com/br. Acesso em: 16 jan. 2026.

IBM SECURITY. Cost of a Data Breach Report 2025. Armonk: IBM, 2025. Disponível em: https://brasil.newsroom.ibm.com/2025-07-30-Relatorio-da-IBM-Custo-medio-de-uma-violacao-de-dados-no-Brasil-atinge-R-7,19-milhoes. Acesso em: 16 jan. 2026.

PARTE III: O Básico que Sustenta o Avançado

CAPÍTULO 5 - CIS como Base da Imunidade Digital

O que vem antes da imunidade

Imunidade pressupõe organismo. Antes de desenvolver anticorpos, é preciso ter corpo. Antes de detectar invasores, é preciso saber o que pertence ao sistema e o que não pertence. A analogia biológica serve bem ao propósito deste capítulo: nenhuma arquitetura de defesa funciona sem fundamentos sobre os quais se apoiar.

O conceito de Imunidade Digital, desenvolvido em profundidade no volume seguinte desta série, parte de uma premissa que parece óbvia, mas raramente é praticada: organizações precisam desenvolver capacidade própria de detectar, responder e aprender com ameaças. Não terceirizar completamente essa função para fornecedores. Não depender exclusivamente de ferramentas automatizadas. Não esperar que alguém de fora avise quando algo estiver errado.

A Imunidade Digital se materializa através de dois mecanismos complementares. O primeiro é o ESC, Escritório de Segurança Corporativa, que não é uma área no organograma nem departamento permanente. É colegiado temporário de colaboradores, multidisciplinar, que se ativa quando necessário e se dissolve quando o problema está resolvido. Não gera custo fixo. Não cria burocracia. Funciona porque coloca as pessoas certas na sala no momento certo.

O segundo mecanismo é o HIDS-BR, Human Intrusion Detection System, framework prático que transforma colaboradores em sensores de segurança. A premissa é simples: você já tem detectores espalhados pela empresa. São seus funcionários. Eles só não sabem que são. Com treinamento mínimo e canal de comunicação adequado, essa rede humana identifica ameaças que nenhum software consegue detectar, precisamente porque ameaças modernas exploram comportamento operacional humano, não apenas vulnerabilidades técnicas.

Ambos os mecanismos são poderosos. Ambos são acessíveis a organizações de qualquer porte. E ambos são completamente inúteis sem uma fundação prévia que este capítulo se propõe a explicar.

A pergunta que paralisa o ESC

Imagine a cena. Um incidente de segurança foi detectado. O ESC é convocado. Representantes de TI, jurídico, comunicação, operações e alta direção se reúnem na sala. A primeira pergunta surge naturalmente: o que foi afetado?

E ninguém consegue responder.

Não porque as pessoas sejam incompetentes. Mas porque a organização nunca construiu um inventário confiável de seus ativos. Ninguém sabe ao certo quantos computadores existem, quais aplicações rodam em cada um, onde estão os dados críticos, quem tem acesso a quê. O ESC, convocado para coordenar resposta, passa as primeiras horas fazendo o trabalho que deveria ter sido feito meses ou anos antes: descobrir o que a empresa possui.

Essa cena não é hipotética. É padrão. Em muitas décadas atuando com segurança corporativa, presenciei variações dela dezenas de vezes. O incidente acontece, o colegiado se forma, e a primeira reunião é consumida por perguntas básicas que deveriam ter respostas prontas.

O CIS Controls, se previamente implementado, resolve esse problema antes que ele aconteça. Não por magia, mas por método. Os dois primeiros controles do framework existem precisamente para garantir que, quando o ESC for convocado, ele tenha informação para trabalhar.

Controle 1: Saber o que você tem (hardware)

O Controle 1 do CIS, "Inventory and Control of Enterprise Assets", parece trivial à primeira leitura. Mantenha inventário de tudo que se conecta à sua rede. Óbvio, não? A trivialidade é ilusória.

A maioria das organizações não sabe quantos dispositivos possui. Não sabe quais estão ativos. Não sabe quais foram autorizados a conectar e quais simplesmente apareceram. Shadow IT, o fenômeno de colaboradores adicionando dispositivos e serviços sem conhecimento de TI, é regra, não exceção. Um estudo da Gartner estimou que organizações desconhecem entre 30% e 40% dos dispositivos conectados às suas redes.

O Safeguard 1.1, primeiro da lista do IG1, exige inventário detalhado e atualizado de todos os ativos corporativos com potencial de armazenar ou processar dados. Inclui dispositivos de usuário final (desktops, laptops, smartphones), dispositivos de rede (roteadores, switches, access points), dispositivos IoT (impressoras, câmeras, sensores) e servidores (físicos, virtuais, em nuvem). O inventário deve registrar endereço de rede, endereço de hardware, nome da máquina, proprietário do ativo, departamento e se o ativo foi aprovado para conectar à rede. Revisão semestral, no mínimo.

O Safeguard 1.2 complementa: processo para endereçar ativos não autorizados semanalmente. Remover da rede, negar conexão remota ou quarentenar. A frequência semanal não é arbitrária. Atacantes que ganham ponto de apoio em redes corporativas frequentemente permanecem meses sem detecção. Verificação semanal reduz a janela de oportunidade.

Para o ESC, essas informações são críticas. Quando o incidente acontece, a primeira pergunta ("o que foi afetado?") tem resposta imediata se o inventário existe e está atualizado. O colegiado pode avançar para contenção em vez de perder horas em descoberta de ativos.

Controle 2: Saber o que roda no que você tem (software)

O Controle 2, "Inventory and Control of Software Assets", segue lógica similar aplicada a software. Se você não sabe quais aplicações rodam em suas máquinas, não sabe quais vulnerabilidades está exposto. Não sabe se há software não autorizado instalado. Não sabe se há versões desatualizadas que deveriam ter sido substituídas.

O Safeguard 2.1 exige inventário detalhado de todo software licenciado instalado em ativos corporativos. Título, publicador, data de instalação, propósito de negócio, versões, mecanismo de deployment. Revisão semestral.

O Safeguard 2.2 é particularmente relevante: garantir que apenas software atualmente suportado esteja designado como autorizado. Software sem suporte do fabricante não recebe mais patches de segurança. Vulnerabilidades descobertas permanecem abertas indefinidamente. Cada aplicação legada rodando em produção é dívida técnica de segurança acumulando juros.

O Safeguard 2.3 fecha o ciclo: processo para endereçar software não autorizado mensalmente. Remover ou documentar exceção. A documentação de exceção é importante. Há situações onde software legado precisa continuar operando por razões de negócio. Nesses casos, a decisão de risco deve ser consciente, documentada e acompanhada de controles compensatórios.

Para o ESC, o inventário de software permite responder à segunda pergunta crítica durante incidentes: qual versão está rodando? Está vulnerável ao exploit que está sendo explorado? Quantos sistemas precisam ser atualizados ou isolados?

Controle 17: A ponte direta com o ESC

Se os Controles 1 e 2 fornecem a matéria-prima informacional para o ESC, o Controle 17, "Incident Response Management", é a interface direta com ele.

O Controle 17 exige que organizações estabeleçam programa para desenvolver e manter capacidade de resposta a incidentes: políticas, planos, procedimentos, papéis definidos, treinamento, comunicações. Os nove safeguards do controle cobrem desde designação de pessoal até condução de revisões pós-incidente.

O Safeguard 17.1 exige designar pessoal para gerenciar o processo de resposta. O Safeguard 17.3 exige estabelecer e manter processo documentado para que a força de trabalho reporte incidentes de segurança. O Safeguard 17.4 exige processo de resposta que enderece papéis, responsabilidades, requisitos de compliance e plano de comunicação. O Safeguard 17.7 exige exercícios periódicos de simulação. Cada um desses elementos encontra correspondência direta na operação do ESC.

A conexão não é acidental. O CIS Controls foi desenvolvido por profissionais que responderam a incidentes reais. Eles sabem que a diferença entre contenção eficaz e desastre prolongado frequentemente reside na preparação prévia. Sabem que improviso sob pressão produz erros. Sabem que documentação atualizada economiza horas críticas nas primeiras fases de resposta.

O ESC sem Controle 17 implementado é colegiado de pessoas bem-intencionadas sem roteiro. O Controle 17 sem estrutura como ESC é documentação que ninguém consulta quando o incidente acontece. A combinação de ambos produz capacidade real de resposta.

O elo que falta: de controles implementados a controles operacionais

Implementar o IG1 é necessário. Não é suficiente.

Uma organização pode executar com disciplina os 56 safeguards essenciais. Pode ter inventário atualizado, acessos controlados, backups testados, sistemas configurados conforme baseline de segurança. Pode, em suma, fazer tudo certo do ponto de vista técnico e processual. E ainda assim descobrir, no momento do incidente, que não sabe o que fazer.

O problema não é o que foi implementado. É quem opera o que foi implementado quando a situação exige decisão.

O CIS Controls define controles. Não define governança de ativação. Estabelece que a organização deve ter processo documentado de resposta a incidentes (Safeguard 17.1), que deve designar pessoal para gerenciar o processo (Safeguard 17.3), que deve conduzir exercícios periódicos (Safeguard 17.7). Mas a operacionalização dessas salvaguardas, o mecanismo concreto que transforma documentação em ação coordenada, permanece fora do escopo do framework.

Para grandes organizações com equipes dedicadas de segurança, esse gap é preenchido por estruturas permanentes: Security Operations Centers, times de resposta a incidentes, hierarquias estabelecidas de escalonamento. PMEs não dispõem desses recursos. E é precisamente aqui que o conceito de ESC se torna relevante.

O ESC não compete com o CIS. Complementa-o. Onde o CIS termina (controles implementados), o ESC começa (controles ativados). O CIS responde à pergunta "o que precisa existir?". O ESC responde à pergunta "quem decide o quê quando algo acontece?".

Para uma PME que implementou o IG1, o ESC funciona como camada de governança que faz os controles valerem. Sem ele, a organização tem os instrumentos mas não tem a orquestra. Tem o plano de resposta documentado mas não tem clareza sobre quem executa cada passo. Tem backup mas não tem certeza de quem autoriza a restauração, em qual ordem, com qual comunicação a stakeholders.

A relação é de dependência mútua. O ESC sem CIS não sabe o que está protegendo (falta inventário), não sabe quem pode o quê (falta controle de acesso), não tem para onde restaurar (falta backup). O CIS sem ESC sabe tudo isso, mas não operacionaliza o que fazer com o conhecimento quando a crise chega.

Imunidade Digital, conceito central do próximo volume, emerge dessa síntese. Não é apenas ter controles (CIS). Não é apenas ter governança de resposta (ESC). É ter ambos operando de forma integrada, onde o conhecimento gerado pelos controles alimenta as decisões da governança, e as decisões da governança ativam os controles no momento certo.

Para o leitor que implementará o IG1 em sua organização, a recomendação é clara: não trate a implementação como projeto finalizado quando os safeguards estiverem operacionais. Reserve esforço equivalente para definir quem, quando, como. O Controle 17 do CIS aponta a direção. O ESC, detalhado no Volume 2 desta série, oferece o mecanismo.

O básico bem feito inclui saber o que fazer com o básico quando ele for testado.

Onde o humano complementa o controle técnico

O CIS Controls v8.1 inclui o Controle 14, "Security Awareness and Skills Training". É controle frequentemente subestimado, tratado como obrigação burocrática a ser cumprida com vídeos genéricos e questionários de múltipla escolha. A abordagem desperdiça oportunidade significativa.

O Safeguard 14.2 exige treinamento para reconhecer ataques de engenharia social: phishing, pretexting, tailgating. O Safeguard 14.6 exige que colaboradores saibam reconhecer potencial incidente e saibam como reportá-lo. Esses safeguards, implementados com seriedade, criam exatamente o que o HIDS-BR formaliza: rede humana de detecção.

A diferença entre cumprir o Controle 14 burocraticamente e implementá-lo como fundação do HIDS-BR está na intencionalidade. Treinamento burocrático ensina

colaboradores a passar no teste. Treinamento orientado para detecção humana ensina colaboradores a observar, questionar e reportar. O primeiro produz métricas de compliance. O segundo produz capacidade defensiva real.

O HIDS-BR parte do reconhecimento de que ameaças modernas são projetadas para contornar controles técnicos. Phishing sofisticado passa por filtros de e-mail. Engenharia social por telefone não deixa logs em sistemas. Manipulação presencial não dispara alertas de firewall. Essas ameaças são detectadas por pessoas, se as pessoas souberem o que observar e tiverem canal para reportar.

O CIS fornece o arcabouço. O HIDS-BR fornece o método. Sem o primeiro, o segundo não tem contexto. Sem o segundo, o primeiro permanece exercício técnico que ignora a superfície de ataque mais explorada: o comportamento humano.

O mínimo defensável da imunidade

Imunidade Digital, como conceito, pode parecer ambiciosa para organizações que ainda lutam com básico. A boa notícia é que o básico, bem feito, já constitui fundação suficiente.

Uma organização que implementou IG1 do CIS Controls possui:

Inventário de ativos de hardware atualizado semestralmente (Safeguard 1.1). Processo para endereçar ativos não autorizados semanalmente (Safeguard 1.2). Inventário de software licenciado (Safeguard 2.1). Verificação de que software autorizado está atualmente suportado (Safeguard 2.2). Processo de gestão de dados que endereça sensibilidade, proprietário, retenção e descarte (Safeguard 3.1). Processo de configuração segura para ativos (Safeguard 4.1). Inventário de contas (Safeguard 5.1). Processo de resposta a incidentes documentado (Safeguard 17.3). Pessoal designado para gerenciar incidentes (Safeguard 17.1).

Essa lista parcial, cobrindo apenas alguns dos 56 safeguards do IG1, demonstra o ponto: uma organização que implementou o nível essencial do CIS já possui a matéria-prima para operar ESC e HIDS-BR. Já sabe o que tem, quem pode o quê, onde estão os dados críticos, como responder quando algo acontece.

A tentação do atalho é compreensível. Controles básicos são trabalhosos. Inventários precisam ser construídos e mantidos. Processos precisam ser documentados e testados. Pessoas precisam ser treinadas e recicladas. É mais excitante falar em "centro de operações de segurança" do que em "planilha de inventário de ativos".

Mas a planilha de inventário, atualizada, é mais útil durante incidente do que centro de operações sofisticado que não sabe o que está monitorando.

O CIS Controls existe para impor essa disciplina. Os Implementation Groups existem para torná-la proporcional. O IG1, com seus 56 safeguards, representa o

investimento mínimo necessário para que qualquer estrutura de resposta funcione. Pular essa etapa não economiza tempo. Transfere o trabalho para o pior momento possível: o meio do incidente.

Construindo a ponte

Este capítulo estabelece conexão que será desenvolvida no próximo volume da série. O CIS Controls não é concorrente do conceito de Imunidade Digital. É seu pré-requisito operacional.

O ESC precisa do CIS para ter informação. O HIDS-BR precisa do CIS para ter contexto. A capacidade organizacional de detectar, responder e aprender com ameaças precisa do CIS para ter fundação sobre a qual se apoiar.

A relação é de dependência, não de escolha. Organizações que tentam desenvolver imunidade digital sem implementar controles básicos constroem castelo sobre areia. A estrutura pode parecer impressionante, mas não sobrevive à primeira tempestade.

O caminho proposto é outro. Começar pelo CIS. Construir inventários. Documentar processos. Treinar pessoas. Estabelecer fundação sólida. Então, sobre essa fundação, erguer estruturas mais sofisticadas de resposta e detecção.

O próximo volume desta série desenvolve esse segundo movimento. Este volume, e especialmente este capítulo, estabelece que sem o primeiro movimento não há segundo. Sem básico bem feito, não há sofisticação possível. Sem CIS implementado, Imunidade Digital é apenas conceito atraente sem capacidade de execução.

Referências do Capítulo

CENTER FOR INTERNET SECURITY. CIS Critical Security Controls Version 8.1. June 2024. Disponível em: https://www.cisecurity.org/controls/v8. Acesso em: jan. 2025.

CENTER FOR INTERNET SECURITY. CIS Controls v8.1 Mapping to NIST CSF 2.0. 2024. Disponível em: https://www.cisecurity.org/controls/v8. Acesso em: jan. 2025.

CENTER FOR INTERNET SECURITY. Guide to Implementation Groups (IG): CIS Critical Security Controls v8.1. November 2024. Disponível em: https://www.cisecurity.org/controls/v8. Acesso em: jan. 2025.

VERIZON. 2024 Data Breach Investigations Report. 2024. Disponível em: https://www.verizon.com/business/resources/reports/dbir/. Acesso em: jan. 2025.

PONEMON INSTITUTE. Cost of a Data Breach Report 2024. IBM Security, 2024. Disponível em: https://www.ibm.com/reports/data-breach. Acesso em: jan. 2025.

CAPÍTULO 6 - CIS e Agentes Invisíveis

O problema que o CIS não previu

Quando o CIS Controls foi concebido, a pergunta fundamental era: quem pode acessar nossos sistemas? A resposta presumia interlocutor humano. Um funcionário, um terceiro, um invasor. Alguém com nome, com intenção, com responsabilidade atribuível.

Essa premissa envelheceu.

No final de 2024, pesquisas de mercado mais antigas já indicavam proporção de dez identidades de máquina para cada identidade humana nas organizações. Projeções para 2026 apontam que essa proporção chegará a oitenta e duas para uma. Para cada pessoa com credenciais nos sistemas da sua empresa, existirão mais de oitenta entidades não humanas com algum tipo de acesso: contas de serviço executando rotinas em servidores, APIs transferindo dados entre plataformas, bots respondendo mensagens, agentes de inteligência artificial tomando decisões que você talvez nem saiba que delegou.

Esses agentes não têm rosto. Não têm crachá. Não aparecem na folha de pagamento. Mas têm credenciais, permissões e capacidade de agir. E quando algo dá errado, a pergunta que ninguém consegue responder com clareza é: quem é o responsável?

O CIS Controls v8.1 não foi desenhado para esse cenário mas pode ser ajustado. Seus controles presumem, em larga medida, que identidades são humanas e que a gestão de acessos se organiza em torno de pessoas. A limitação não invalida o framework. Apenas exige que entendamos onde ele termina e onde extensões se tornam necessárias.

Este capítulo explora essa fronteira.

O que são agentes invisíveis

Antes de discutir como o CIS se relaciona com o problema, é preciso delimitar o problema.

Agentes invisíveis, no contexto desta série, são entidades não humanas que operam em nome de pessoas ou organizações, com capacidade de acessar sistemas, processar dados e executar ações. O termo abrange categorias tecnicamente distintas mas operacionalmente convergentes.

Contas de serviço são credenciais criadas para que aplicações e processos automatizados acessem recursos do sistema. Não pertencem a pessoas específicas.

Frequentemente são criadas durante instalação de software e depois esquecidas, acumulando permissões que ninguém revisa.

API keys são tokens de autenticação que permitem comunicação entre sistemas. Quando o sistema de vendas consulta o sistema de estoque, uma API key autentica essa comunicação. O problema surge quando essas chaves são criadas sem controle, compartilhadas entre ambientes, ou nunca rotacionadas.

Tokens de acesso são credenciais temporárias ou permanentes que autorizam ações específicas. OAuth tokens, JWT tokens, bearer tokens. Proliferam em arquiteturas modernas e frequentemente operam com permissões excessivas porque configurar o mínimo necessário exige esforço que ninguém quer investir.

Bots e automações são scripts e programas que executam tarefas repetitivas. O bot que responde mensagens no WhatsApp corporativo. O script que processa faturas automaticamente. A automação que move arquivos entre pastas. Cada um opera com credenciais próprias, cada um representa superfície de ataque potencial.

Agentes de IA são a categoria mais recente e mais problemática. Diferentemente de bots tradicionais que seguem regras predefinidas, agentes de IA interpretam contexto, tomam decisões e executam ações complexas com autonomia variável. Um agente que agenda reuniões precisa acessar calendários. Um agente que responde e-mails precisa ler e escrever mensagens. Um agente que analisa documentos precisa acessar repositórios. Cada capacidade implica permissões. Cada permissão implica risco.

O denominador comum é invisibilidade. Essas entidades não aparecem em organogramas. Não participam de reuniões. Não recebem treinamento de segurança. Não são demitidas quando mudam de função. Operam continuamente, silenciosamente, frequentemente sem que ninguém saiba exatamente o que fazem ou quais permissões possuem.

Onde o CIS alcança

O CIS Controls não ignora completamente identidades não humanas. Alguns controles endereçam diretamente aspectos do problema, ainda que com vocabulário e enquadramento voltados para contexto mais tradicional.

O Controle 5, "Account Management", estabelece fundamentos aplicáveis. O Safeguard 5.1 exige inventário de todas as contas gerenciadas pela empresa, incluindo implicitamente contas de serviço. O Safeguard 5.5 vai além: exige inventário específico de contas de serviço, com registro de proprietário departamental, data de revisão e propósito. Revisões trimestrais são mandatórias para validar que contas ativas permanecem autorizadas.

A exigência é significativa. Organizações que implementam o Safeguard 5.5 com rigor descobrem contas de serviço criadas anos antes por funcionários que já saíram da empresa, para propósitos que ninguém lembra, com permissões que ninguém ousou revisar. O inventário força visibilidade. Visibilidade é pré-requisito para controle.

O Controle 6, "Access Control Management", complementa com gestão de permissões. O Safeguard 6.1 estabelece processo documentado para concessão de acessos. O Safeguard 6.2 estabelece processo para revogação. Ambos se aplicam a contas de serviço tanto quanto a contas humanas. O Safeguard 6.8, exclusivo do IG3, exige definição e manutenção de controle de acesso baseado em papéis (role-based access control), com revisões anuais para validar que privilégios permanecem autorizados.

O Controle 3, "Data Protection", importa porque agentes invisíveis frequentemente processam dados sensíveis. O Safeguard 3.3 exige configuração de listas de controle de acesso baseadas em necessidade de conhecimento. Quando uma API acessa banco de dados de clientes, as permissões dessa API precisam refletir o mínimo necessário para sua função. Na prática, APIs frequentemente operam com permissões de administrador porque era mais fácil configurar assim.

O Controle 8, "Audit Log Management", é onde visibilidade se torna rastreabilidade. O Safeguard 8.5 exige logs detalhados para ativos que contêm dados sensíveis, incluindo origem do evento, data, usuário, timestamp, endereços de origem e destino. Quando "usuário" é conta de serviço ou API, o log precisa registrar isso de forma que permita reconstrução posterior de quem fez o quê, quando e por quê.

Esses controles, implementados com seriedade, criam fundação para governança de identidades não humanas. O problema é que a maioria das organizações não os implementa pensando em agentes invisíveis. Implementa pensando em pessoas, e as lacunas aparecem.

Onde o CIS não alcança

Os limites do framework tornam-se evidentes quando examinamos o que ele não endereça.

O CIS não distingue entre tipos de identidades não humanas. Conta de serviço, API key, token OAuth, agente de IA: para o framework, são todas "contas" a serem inventariadas e gerenciadas. A simplificação é problemática porque cada tipo apresenta características e riscos distintos. Uma conta de serviço tradicional opera dentro de perímetro definido. Um agente de IA pode navegar na web, interagir com sistemas externos, tomar decisões que seus criadores não anteciparam.

O CIS não endereça ciclo de vida de credenciais não humanas com a especificidade necessária. Quando um funcionário sai da empresa, o processo de

desligamento inclui revogação de acessos. Quando uma integração é desativada, quem revoga as API keys? Quando um projeto piloto de automação é abandonado, quem descomissiona as contas de serviço? O framework exige processos de revogação, mas não oferece orientação específica para o contexto não humano.

O CIS não trata de permissões dinâmicas e contextuais. Agentes de IA modernos frequentemente operam com permissões que variam conforme contexto. O agente pode ter permissão para ler e-mails, mas apenas e-mails de determinado remetente. Pode ter permissão para agendar reuniões, mas apenas em determinados horários. Essa granularidade excede o que o framework tradicional de controle de acesso contempla.

O CIS não endereça a questão de responsabilização algorítmica. Quando um agente de IA toma decisão que causa dano, quem responde? O desenvolvedor que criou o agente? O gestor que autorizou seu uso? O fornecedor da plataforma? O framework oferece controles técnicos, não respostas para dilemas de responsabilidade que ainda estão sendo debatidos em tribunais e reguladores.

O CIS não contempla agentes que aprendem e evoluem. Um script tradicional faz hoje o mesmo que fazia ontem. Um agente de IA baseado em aprendizado de máquina pode modificar seu comportamento com base em dados que processa. Essa capacidade evolutiva desafia premissas de controle baseadas em comportamento previsível e documentável.

A extensão necessária

Reconhecer os limites do CIS não significa abandoná-lo. Significa usá-lo como fundação sobre a qual extensões específicas são construídas.

O inventário de ativos (Controles 1 e 2) precisa ser expandido para incluir mapeamento de onde agentes invisíveis operam. Quais servidores hospedam contas de serviço? Quais aplicações utilizam APIs externas? Quais departamentos implementaram automações? O inventário tradicional de hardware e software é pré-requisito, mas não substituto para inventário específico de identidades não humanas.

O inventário de contas (Safeguard 5.5) precisa ser detalhado além do que o CIS especifica. Para cada conta de serviço, API key ou token, a organização precisa documentar: quem criou, quando, para qual propósito, com quais permissões, com qual prazo de validade, quem é responsável por revisão periódica, qual processo de descomissionamento se aplica. Esse nível de detalhe excede o que o CIS exige, mas é necessário para governança efetiva.

O controle de acesso (Controle 6) precisa incorporar princípio de privilégio mínimo com rigor que a prática raramente alcança. Cada agente invisível deve operar com as permissões mínimas necessárias para sua função específica. Não com permissões de administrador porque era mais fácil. Não com acesso a todos os dados

porque ninguém quis configurar restrições. Mínimo necessário, documentado, revisado, ajustado quando função muda.

O monitoramento (Controle 8) precisa ser capaz de distinguir atividade normal de atividade anômala para cada agente. Isso exige baseline comportamental: o que essa conta de serviço normalmente faz, em quais horários, acessando quais recursos? Desvios do baseline são alertas. Sem baseline, não há como detectar que a API que normalmente processa cem transações por hora subitamente processou dez mil.

O gerenciamento de resposta a incidentes (Controle 17) precisa incluir playbooks específicos para incidentes envolvendo identidades não humanas. Se uma API key é comprometida, qual é o processo de revogação emergencial? Se um agente de IA começa a se comportar de forma inesperada, como é desativado? Quem tem autoridade para tomar essas decisões fora do horário comercial?

O risco de não estender

Organizações que implementam CIS Controls sem considerar agentes invisíveis operam com falsa sensação de segurança. Os controles humanos estão funcionando. Os inventários de pessoas estão atualizados. Os processos de concessão e revogação para funcionários estão documentados. Enquanto isso, dezenas ou centenas de identidades não humanas operam sem inventário, sem revisão, sem responsabilização.

O cenário de incidente é previsível. Atacante compromete API key exposta em repositório de código. Usa a key para acessar sistemas internos. Move-se lateralmente usando permissões excessivas que a API nunca deveria ter tido. Exfiltra dados durante meses porque ninguém monitora o que aquela API normalmente faz. Quando o incidente é descoberto, a pergunta "como isso aconteceu?" revela que ninguém sabia que aquela API existia, quem a criou, ou por que tinha acesso aos dados comprometidos.

A responsabilização se torna complexa. A organização implementou CIS Controls. Passou em auditorias. Demonstrou diligência. Mas os controles presumiam interlocutor humano, e o vetor de ataque foi não humano. O regulador pergunta: vocês tinham inventário de API keys? Vocês revisavam permissões de contas de serviço? Vocês monitoravam comportamento de automações? As respostas, frequentemente, são variações de "não pensamos nisso".

O terceiro volume desta série, dedicado integralmente ao tema de Agentes Invisíveis, desenvolve framework completo para governança de identidades não humanas. Este capítulo estabelece a ponte: o CIS é fundação necessária, mas não suficiente. Sem inventário de ativos, não há como saber onde agentes operam. Sem gestão de contas, não há como rastrear quais agentes existem. Sem controle de

acesso, não há como limitar o que agentes podem fazer. Sem logs, não há como investigar o que agentes fizeram.

O CIS fornece o esqueleto. A governança de agentes invisíveis adiciona o que o esqueleto não contempla.

O fator velocidade

Uma característica dos agentes invisíveis merece atenção específica: velocidade de proliferação.

Criar conta de usuário para novo funcionário exige processo de RH, aprovações, configurações. O processo natural impõe fricção que limita velocidade. Criar API key pode ser feito por desenvolvedor em segundos, sem aprovação, sem registro, sem processo. A assimetria é perigosa.

O Safeguard 5.5 exige revisão trimestral de contas de serviço. Em três meses, quantas novas integrações foram criadas? Quantas API keys foram geradas? Quantos agentes de automação foram implementados por usuários de negócio usando plataformas no-code? A revisão trimestral pode encontrar dezenas de novas identidades não humanas que surgiram desde a última revisão, cada uma sem documentação de propósito, proprietário ou permissões adequadas.

A solução não é proibir criação de identidades não humanas. É impor processo equivalente ao que existe para identidades humanas. Toda nova conta de serviço precisa de aprovação documentada. Toda nova API key precisa de proprietário designado. Todo novo agente precisa de avaliação de permissões antes de entrar em produção. O CIS fornece princípios. A organização precisa adaptar processos.

Plataformas de automação no-code e low-code agravam o desafio. Quando usuários de negócio podem criar automações sem envolvimento de TI, a proliferação de agentes escapa completamente dos controles tradicionais. O departamento de marketing cria bot para postar em redes sociais. O departamento financeiro cria automação para processar faturas. O departamento de vendas cria integração com CRM externo. Cada um opera com credenciais próprias, frequentemente com permissões que ninguém na área de segurança sequer sabe que existem.

Começando pelo que é possível

Diante da complexidade, a tentação é postergar. Esperar que o mercado desenvolva soluções. Esperar que reguladores estabeleçam requisitos claros. Esperar que alguém resolva o problema antes que ele precise ser enfrentado.

A espera é arriscada. Agentes invisíveis já operam em sua organização. Já têm permissões. Já acessam dados. Já representam superfície de ataque. A questão não é se você terá que lidar com isso, mas quando: proativamente, com tempo para planejar, ou reativamente, no meio de um incidente.

O caminho pragmático começa pelo CIS implementado com consciência de suas extensões necessárias.

Implementar Safeguard 5.5 com rigor, tratando inventário de contas de serviço como prioridade, não como formalidade. Expandir o inventário para incluir API keys, tokens e credenciais de automação, mesmo que o CIS não exija explicitamente. Documentar proprietário, propósito e permissões para cada identidade não humana identificada. Estabelecer processo de aprovação para criação de novas identidades não humanas. Configurar alertas para atividade anômala de contas de serviço e APIs críticas.

Esse baseline não resolve o problema completo. Mas cria visibilidade onde antes havia cegueira. Cria processo onde antes havia improviso. Cria fundação sobre a qual governança mais sofisticada pode ser construída.

O CIS Controls, nesse contexto, funciona como ponto de partida, não como destino. Implementá-lo é necessário. Parar nele é insuficiente. A jornada continua no terceiro volume desta série, onde o tema de Agentes Invisíveis recebe tratamento completo que suas complexidades exigem.

Referências do Capítulo

CENTER FOR INTERNET SECURITY. CIS Critical Security Controls Version 8.1. June 2024. Disponível em: https://www.cisecurity.org/controls/v8. Acesso em: jan. 2025.

CYBERARK. 2024 Identity Security Threat Landscape Report. 2024. Disponível em: https://www.cyberark.com/resources/threat-landscape-report. Acesso em: jan. 2025.

PERMISO. Non-Human Identity (NHI) Security Guide. 2024. Disponível em: https://permiso.io/non-human-identity-nhi-security-guide. Acesso em: jan. 2025.

OWASP. API Security Top 10. 2023. Disponível em: https://owasp.org/API-Security/. Acesso em: jan. 2025.

GARTNER. Managing Machine Identities, Secrets, Keys and Certificates. 2024. Disponível em: https://www.gartner.com/en/documents/4017119. Acesso em: jan. 2025.

NEURALTRUST. 5 Predictions for AI Agent Security in 2026. 2025. Disponível em: https://neuraltrust.ai/blog/5-predictions-for-ai-agents-security-in-2026. Acesso em: jan. 2025.

CAPÍTULO 7 - CIS e Ameaças Quânticas

O horizonte que parece distante

Computação quântica soa como ficção científica. Qubits, superposição, emaranhamento. Termos que parecem pertencer a laboratórios de física, não a reuniões de diretoria. A tentação natural é classificar o tema como preocupação futura, problema para a próxima geração de executivos resolver.

A tentação é perigosa.

Enquanto computadores quânticos capazes de quebrar criptografia atual ainda não existem em escala prática, uma ameaça derivada já opera no presente. Chama-se “Harvest Now, Decrypt Later”: adversários capturam dados criptografados hoje, armazenam pacientemente, e aguardam o momento em que capacidade quântica permitirá descriptografá-los. Governos hostis, grupos de espionagem industrial, organizações criminosas sofisticadas. Eles não conseguem ler seus dados agora. Mas estão guardando.

A implicação é direta: dados criptografados hoje com algoritmos vulneráveis a ataques quânticos permanecerão vulneráveis indefinidamente. Contratos confidenciais assinados em 2024 poderão ser lidos em 2030 ou antes. Segredos industriais protegidos este ano poderão ser expostos na próxima década. Informações pessoais de clientes coletadas agora poderão ser devassadas quando a tecnologia amadurecer.

O quarto volume desta série dedica-se integralmente ao tema, com profundidade que este capítulo não pretende replicar. O propósito aqui é mais específico: demonstrar que a preparação para ameaças quânticas começa com controles básicos bem executados. Sem CIS implementado, a transição para criptografia pós-quântica é inviável. O básico, mais uma vez, precede o avançado.

O que a ameaça quântica exige

Preparar-se para ameaças quânticas não significa comprar produtos rotulados como "quantum-safe". Significa desenvolver capacidade organizacional de identificar onde a criptografia vulnerável está em uso e substituí-la de forma ordenada quando necessário. Essa capacidade tem nome técnico: “crypto-agility”, ou agilidade criptográfica.

Crypto-agility é a habilidade de trocar algoritmos criptográficos sem reescrever sistemas inteiros. Parece simples. Na prática, é extraordinariamente difícil para organizações que não conhecem seu próprio ambiente.

A dificuldade começa com uma pergunta aparentemente básica: onde usamos criptografia? A resposta, para a maioria das organizações, é variação de "em muitos lugares, provavelmente". Criptografia está embutida em protocolos de comunicação, em certificados digitais, em conexões com bancos de dados, em integrações com parceiros, em bibliotecas de software, em configurações de servidores. Está em lugares que ninguém lembra que existe, configurada por pessoas que já saíram da empresa, usando algoritmos que ninguém sabe nomear.

A segunda pergunta é igualmente desafiadora: quais algoritmos estamos usando? RSA-2048? Curvas elípticas? AES-128? SHA-192? Cada algoritmo tem perfil de vulnerabilidade diferente frente a ataques quânticos. Alguns precisarão ser substituídos. Outros permanecerão seguros. Sem saber quais algoritmos estão em uso e onde, a organização não consegue priorizar a transição.

A terceira pergunta fecha o ciclo: quais dados precisam de proteção de longo prazo? Informações que perdem relevância em meses não precisam de criptografia resistente a ataques que talvez ocorram em década. Informações que precisam permanecer confidenciais por vinte, trinta, cinquenta anos exigem proteção diferente. A priorização depende de conhecer os dados e sua vida útil de confidencialidade.

Nenhuma dessas perguntas pode ser respondida sem fundações que o CIS Controls estabelece.

Inventário como pré-requisito

O Controle 1, inventário de ativos de hardware, e o Controle 2, inventário de ativos de software, são onde a preparação quântica começa, mesmo que o CIS não mencione computação quântica em lugar algum.

A lógica é derivativa. Criptografia não existe no abstrato. Existe em sistemas específicos, rodando em hardware específico, executando software específico. Sem saber quais sistemas existem, não há como mapear onde criptografia está em uso. Sem saber qual software roda nesses sistemas, não há como identificar quais bibliotecas criptográficas estão instaladas. O inventário de ativos é fundação sobre a qual inventário criptográfico pode ser construído.

O inventário criptográfico não é exigência explícita do CIS v8.1. É extensão natural dos Controles 1 e 2 quando o contexto de ameaças quânticas é considerado. Para cada sistema no inventário, a organização precisa identificar: quais protocolos criptográficos estão em uso, quais algoritmos esses protocolos implementam, quais bibliotecas fornecem as funções criptográficas, quando certificados digitais expiram, quem é responsável por atualizações.

Organizações que não têm inventário básico de ativos não conseguem construir inventário criptográfico. Organizações que não têm inventário criptográfico

não conseguem planejar migração para algoritmos pós-quânticos. A cadeia de dependências é clara: sem Controle 1 e 2 implementados, crypto-agility é impossível.

Onde algoritmos vulneráveis se escondem

O Controle 4, "Secure Configuration of Enterprise Assets and Software", ganha relevância específica no contexto quântico. Configuração segura, no CIS, significa eliminar configurações padrão inseguras, desabilitar serviços desnecessários, aplicar hardening (tornar as configurações seguras). No contexto quântico, significa também identificar onde configurações criptográficas vulneráveis persistem.

Algoritmos criptográficos vulneráveis frequentemente se escondem em lugares inesperados.

Protocolos de comunicação legados mantêm suporte a algoritmos antigos por compatibilidade retroativa. Um servidor pode suportar TLS 1.3 com algoritmos modernos, mas também aceitar conexões TLS 1.0 com algoritmos que eram padrão há quinze anos. A configuração existe para não quebrar integração com sistema legado que ninguém quer atualizar. Cada compatibilidade retroativa é superfície de ataque potencial.

Certificados digitais podem usar algoritmos de assinatura que se tornarão vulneráveis. Certificados emitidos com RSA-2048 ou curvas elípticas tradicionais precisarão ser substituídos. Organizações que não rastreiam seus certificados, suas datas de expiração e seus algoritmos de assinatura descobrirão a necessidade de substituição no pior momento possível.

Bibliotecas de software embarcam implementações criptográficas que desenvolvedores raramente examinam. Quando aplicação usa biblioteca para "criptografar dados", o desenvolvedor frequentemente não sabe qual algoritmo a biblioteca usa por padrão, se o algoritmo é configurável, ou como seria a migração para algoritmo diferente. A dependência está enterrada em camadas de abstração.

Integrações com parceiros e fornecedores podem impor restrições criptográficas. Se o parceiro só aceita conexões usando determinado protocolo com determinado algoritmo, a organização fica refém dessa configuração até que o parceiro atualize. Mapeamento de dependências criptográficas externas é parte do inventário necessário.

O Controle 4 não menciona criptografia quântica. Mas sua implementação rigorosa força exame de configurações que revelam onde algoritmos vulneráveis estão em uso. Hardening de sistemas inclui desabilitar protocolos e algoritmos obsoletos. A disciplina de configuração segura é, inadvertidamente, preparação para transição quântica.

Proteção de dados e o fator tempo

O Controle 3, "Data Protection", é onde a dimensão temporal da ameaça quântica se manifesta.

O Safeguard 3.1 exige processo de gestão de dados que enderece sensibilidade, proprietário, tratamento, limites de retenção e requisitos de descarte. O Safeguard 3.7 exige esquema de classificação de dados. Essas exigências, no contexto tradicional, servem para garantir que dados sensíveis recebam proteção proporcional. No contexto quântico, servem para identificar quais dados precisam de proteção de longo prazo.

A pergunta crítica é: por quanto tempo esses dados precisam permanecer confidenciais?

Dados de transações financeiras do mês passado têm vida útil de confidencialidade limitada. Dados de propriedade intelectual podem precisar de proteção por décadas. Dados de saúde de pacientes precisam permanecer confidenciais indefinidamente. Segredos industriais que fundamentam vantagem competitiva não têm data de expiração.

Organizações que implementaram Controle 3 com seriedade têm classificação de dados que permite responder essa pergunta. Sabem quais dados são sensíveis, onde estão armazenados, quem é responsável por eles. A partir dessa base, podem adicionar dimensão temporal: quais desses dados sensíveis precisam de proteção que sobreviva à era quântica?

Organizações sem classificação de dados não conseguem priorizar. Tratam todos os dados igualmente, o que significa proteger inadequadamente os mais críticos ou desperdiçar recursos protegendo excessivamente os menos relevantes. A ausência de Controle 3 implementado torna planejamento de transição quântica exercício de adivinhação.

Gestão de mudanças e a migração inevitável

A transição para criptografia pós-quântica não será evento único. Será processo prolongado de substituição gradual, sistema por sistema, integração por integração, certificado por certificado. Processo dessa magnitude exige capacidade de gestão de mudanças que muitas organizações não possuem.

O CIS Controls não tem controle específico dedicado a gestão de mudanças. Mas vários safeguards pressupõem essa capacidade. O Safeguard 4.1 exige processo documentado de configuração segura, o que implica processo para alterar configurações de forma controlada. O Safeguard 7.3 e 7.4 exigem gestão automatizada de patches, o que implica processo para aplicar atualizações sem

quebrar sistemas. O Safeguard 12.3 exige gestão segura de infraestrutura de rede, incluindo controle de versão.

Migração criptográfica é, essencialmente, gestão de mudanças em escala. Trocar algoritmo em um sistema pode quebrar integração com outro sistema. Atualizar biblioteca criptográfica pode introduzir incompatibilidades. Substituir certificado pode invalidar configurações de parceiros. Cada mudança precisa ser planejada, testada, documentada, reversível.

Organizações que já operam com disciplina de gestão de mudanças terão transição mais suave. Organizações que aplicam patches de forma ad hoc, que modificam configurações sem documentação, que não testam alterações antes de produção, enfrentarão migração caótica com interrupções de serviço e retrabalho.

O CIS não prepara especificamente para migração quântica. Mas a disciplina operacional que ele impõe é exatamente o que migração quântica exigirá.

O papel do Controle 15

O Controle 15, "Service Provider Management", adquire relevância específica no contexto de preparação quântica.

Organizações modernas não controlam toda sua infraestrutura criptográfica. Provedores de nuvem gerenciam criptografia de dados armazenados. Provedores de SaaS gerenciam criptografia de aplicações. Processadores de pagamento gerenciam criptografia de transações. Parceiros de integração gerenciam criptografia de comunicações.

O Safeguard 15.1 exige inventário de provedores de serviço. O Safeguard 15.4 exige que contratos incluam requisitos de segurança. No contexto quântico, esses safeguards fundamentam perguntas que precisam ser feitas a cada provedor: qual é sua estratégia de migração para criptografia pós-quântica? Quando você planeja implementar algoritmos quantum-safe? Como você comunicará mudanças que afetam nossos dados?

Provedores que não têm respostas para essas perguntas representam risco. Se o provedor de nuvem onde seus dados mais sensíveis estão armazenados não tem plano de transição quântica, a vulnerabilidade é sua, não dele. Seus dados, seu risco, sua responsabilidade de perguntar.

O Safeguard 15.6, exclusivo do IG3, exige monitoramento de provedores consistente com política de gestão. No contexto quântico, monitoramento inclui acompanhar anúncios de provedores sobre suporte a novos algoritmos, avaliar roadmaps de migração, verificar se compromissos contratuais estão sendo cumpridos.

Organizações que não implementaram Controle 15 não têm visibilidade sobre onde sua criptografia é gerenciada por terceiros. Sem essa visibilidade, não há como avaliar exposição nem como exigir preparação de parceiros.

Começar pelo básico, evoluir com propósito

A mensagem deste capítulo é consistente com a mensagem de toda esta obra: o básico precede o avançado.

Preparação para ameaças quânticas parece tema sofisticado, domínio de especialistas em criptografia e física. Na prática, começa com perguntas fundamentais: sabemos quais sistemas temos? Sabemos qual software roda neles? Sabemos quais dados são sensíveis? Sabemos quais provedores gerenciam nossa infraestrutura?

Organizações que respondem "não" a essas perguntas não estão prontas para discutir criptografia pós-quântica. Estão prontas para implementar CIS Controls.

Organizações que respondem "sim" têm fundação para o próximo passo: construir inventário criptográfico sobre o inventário de ativos, identificar dados que precisam de proteção de longo prazo, mapear dependências de terceiros, desenvolver plano de migração proporcional ao risco.

O quarto volume desta série desenvolve esse próximo passo em profundidade. Este capítulo estabelece que o próximo passo não é possível sem o primeiro. Sem CIS implementado, crypto-agility é aspiração sem fundamento. Com CIS implementado, crypto-agility é extensão natural de capacidades já desenvolvidas.

A ameaça quântica é real e o horizonte está mais próximo do que parece confortável. Mas a resposta não começa com algoritmos exóticos. Começa com inventário de ativos. Começa com classificação de dados. Começa com gestão de provedores. Começa, como tudo em segurança bem-feita, pelo básico.

Referências do Capítulo

CENTER FOR INTERNET SECURITY. CIS Critical Security Controls Version 8.1. June 2024. Disponível em: https://www.cisecurity.org/controls/v8. Acesso em: jan. 2025.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. Post-Quantum Cryptography. 2024. Disponível em: https://csrc.nist.gov/projects/post-quantum-cryptography. Acesso em: jan. 2025.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard. August 2024. Disponível em: https://csrc.nist.gov/publications/detail/fips/203/final. Acesso em: jan. 2025.

EUROPEAN UNION AGENCY FOR CYBERSECURITY. Post-Quantum Cryptography: Current State and Quantum Mitigation. 2024. Disponível em: https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation. Acesso em: jan. 2025.

MOSCA, Michele. Cybersecurity in an Era with Quantum Computers: Will We Be Ready? IEEE Security & Privacy, v. 16, n. 5, p. 38-41, 2018. Disponível em: https://ieeexplore.ieee.org/document/8490171. Acesso em: jan. 2025.

CLOUD SECURITY ALLIANCE. Practical Preparations for the Post-Quantum World. 2024. Disponível em: https://cloudsecurityalliance.org/research/working-groups/quantum-safe-security/. Acesso em: jan. 2025.

PARTE IV: Como Usar o CIS sem virar Refém dele

CAPÍTULO 8 - Implementação Proporcional por Perfil

A falácia do tamanho único

Frameworks de segurança costumam ser escritos como se todos os leitores fossem iguais. Documentação técnica presume conhecimento técnico. Guias executivos presume autoridade decisória. Checklists de compliance presumem contexto regulatório específico. O resultado é que cada leitor precisa traduzir o material para sua realidade, frequentemente sem ferramentas para fazê-lo.

Este capítulo recusa essa abordagem.

O CIS Controls serve públicos distintos com necessidades distintas. O executivo que precisa aprovar orçamento não precisa entender detalhes de configuração. O gestor de TI que precisa implementar controles não precisa de argumentos para convencer o conselho. O advogado que avalia exposição regulatória não precisa de comandos de terminal. O empresário de PME que opera sozinho precisa de tudo isso condensado no essencial.

As próximas seções oferecem orientação específica para cada perfil. Não são receitas completas. São pontos de partida calibrados para diferentes posições na estrutura organizacional e diferentes níveis de autoridade sobre decisões de segurança.

A premissa é simples: segurança proporcional começa por entender o que cada pessoa pode e deve fazer a partir de onde está.

Para Executivos e Conselheiros

Você não precisa entender como firewalls funcionam. Precisa entender se sua organização tem um e se ele está configurado adequadamente. A distinção é crucial. Seu papel não é implementar controles. É garantir que controles sejam implementados, cobrar evidências de que funcionam, e assumir responsabilidade quando falham.

O que você precisa saber

O CIS Controls existe e é referência reconhecida por auditores, reguladores e seguradoras. No Brasil o CIS Controls é reconhecido e explicitamente referenciado por órgãos e iniciativas oficiais brasileiras, sobretudo no governo federal e em guias ligados a tribunais de contas. Não é uma “norma brasileira”, mas aparece como

framework recomendado e usado como base de cursos GOV.BR, guias e modelos de controle.

Sua organização deveria estar implementando, no mínimo, o IG1, o baseline de 56 safeguards que constitui higiene cibernética essencial. A ausência desses controles básicos, em caso de incidente, será tratada como negligência por qualquer avaliador externo. Você, pessoalmente, pode ser responsabilizado se ficar demonstrado que tinha conhecimento dos riscos e não agiu.

O capítulo 3 desta obra detalhou a relação entre CIS e diligência razoável. A síntese para seu contexto: implementar CIS não garante que incidentes não ocorrerão, mas demonstra que a organização tomou medidas proporcionais para preveni-los. Essa demonstração é o que separa negligência de infortúnio aos olhos de tribunais e reguladores.

Perguntas essenciais para fazer ao responsável por TI

Temos inventário atualizado de todos os dispositivos conectados à nossa rede? A resposta deveria ser sim, com data da última atualização. Se a resposta for "mais ou menos" ou "estamos trabalhando nisso", você tem problema.

Temos inventário de todo software instalado em nossos sistemas? Mesma lógica. Sem inventário de software, a organização não sabe o que precisa ser atualizado quando vulnerabilidades são descobertas.

Quanto tempo levamos para aplicar atualizações de segurança críticas? A resposta ideal é "dias". Se a resposta for "semanas" ou "depende", pergunte por que e o que seria necessário para acelerar.

Temos processo documentado para responder a incidentes de segurança? A resposta deveria incluir quem é responsável, como a equipe é acionada, e quando foi o último teste ou simulação. Se nunca houve teste, o processo existe apenas no papel.

Quais dados sensíveis armazenamos e onde estão? Se o responsável por TI não conseguir responder com precisão, a organização não sabe o que precisa proteger com prioridade.

Estamos em conformidade com algum framework de segurança? Se a resposta for CIS Controls, pergunte qual Implementation Group e qual o percentual de safeguards implementados. Se a resposta for "não formalmente", pergunte por que não e o que seria necessário.

Indicadores de que algo está errado

Respostas evasivas ou excessivamente técnicas às perguntas acima. Se você não consegue entender a resposta, ou a resposta não é direta, há problema de comunicação ou problema real sendo ocultado.

Ausência de métricas. Segurança que funciona produz números: quantos dispositivos, quantas vulnerabilidades abertas, quanto tempo para correção, quantos incidentes no período. Ausência de números indica ausência de controle.

Pedidos de orçamento sem justificativa de risco. Investimento em segurança deveria ser apresentado em termos de risco mitigado, não em termos de funcionalidades técnicas. Se a justificativa é "precisamos porque é importante", a comunicação está falhando.

Surpresas recorrentes. Se você só ouve sobre problemas de segurança quando já são crises, a estrutura de reporte não está funcionando. Deveria haver comunicação periódica sobre postura de segurança, não apenas alertas emergenciais.

Responsabilidades pessoais e como se proteger

Documente seu envolvimento. Atas de reuniões onde segurança foi discutida, e-mails solicitando informações, aprovações de orçamento para iniciativas de segurança. Em caso de incidente, essa documentação demonstra que você exerceu supervisão ativa.

Exija reportes periódicos. Segurança deveria ser item de pauta recorrente, não assunto tratado apenas quando há problema. Frequência trimestral é mínimo razoável para organizações de médio porte.

Questione e registre as respostas. Quando o responsável por TI disser que determinado risco é aceitável, peça que documente por escrito. A formalização força reflexão e cria registro de que a decisão foi consciente.

Não ignore alertas. Se alguém na organização levantou preocupação sobre segurança e você não agiu, essa omissão pode ser usada contra você posteriormente.

Alertas merecem investigação, mesmo quando parecem exagerados.

Para Gestores de TI e Segurança

Você está no meio. Entende os problemas técnicos, mas não tem autoridade para resolver todos sozinho. Precisa de orçamento que outros aprovam, de

colaboração de áreas que têm outras prioridades, de atenção de executivos que têm outras preocupações. Sua habilidade mais crítica não é técnica. É comunicação.

Como comunicar necessidades ao alto escalão

Traduza técnico em impacto de negócio. "Precisamos de ferramenta de gestão de vulnerabilidades" é pedido técnico. "Sem gestão de vulnerabilidades, não conseguimos saber em quanto tempo corrigimos falhas críticas, o que nos expõe a ataques e pode afetar renovação do seguro cyber" é argumento de negócio para organizações sérias.

Use o CIS como referência externa. Quando você diz que algo é necessário, pode parecer opinião pessoal. Quando o CIS Controls, adotado globalmente, diz que é necessário, torna-se padrão de mercado. O framework empresta autoridade externa às suas recomendações.

Quantifique sempre que possível. Número de dispositivos sem inventário. Número de vulnerabilidades críticas abertas há mais de 30 dias. Tempo médio para aplicar patches. Percentual de safeguards do IG1 implementados. Números criam objetividade e permitem acompanhamento de progresso.

Apresente opções com trade-offs (alternativas). Em vez de pedir aprovação para uma solução específica, apresente alternativas com diferentes níveis de investimento e proteção. "Podemos fazer A com custo X e proteção Y, ou B com custo maior e proteção maior. Recomendo A porque..." Isso demonstra análise e facilita decisão.

Conecte com eventos externos. Quando incidente de segurança relevante aparece na mídia, use como gancho para discutir se a organização está protegida contra ameaça similar. Não de forma alarmista, mas como oportunidade de verificação.

Priorização quando recursos são limitados

Comece pelo IG1. Os 56 safeguards do Implementation Group 1 foram selecionados especificamente para oferecer máxima proteção com recursos mínimos. Antes de investir em soluções sofisticadas, garanta que o básico está coberto.

Dentro do IG1, priorize por dependência. Inventário de ativos (Controles 1 e 2) é fundação para quase tudo. Sem saber o que você tem, não consegue proteger o que tem. Gestão de contas (Controle 5) e controle de acesso (Controle 6) são próximos, porque credenciais comprometidas são vetor principal de ataques. Proteção contra malware (Controle 10) e recuperação de dados (Controle 11) completam o núcleo essencial.

Use a régua do "e se". Para cada safeguard não implementado, pergunte: se formos atacados explorando essa lacuna, conseguimos explicar por que não estava implementado? Se a explicação for convincente (custo desproporcional, risco baixo, controle compensatório), a priorização faz sentido. Se a explicação for fraca, suba a prioridade.

Documente decisões de não fazer. Quando você decide não implementar determinado safeguard por limitação de recursos, registre a decisão, a justificativa e os riscos aceitos. Essa documentação protege você e a organização, demonstrando que a lacuna é consciente, não ignorância.

Documentação que protege a organização e o profissional

Mantenha registro de implementação. Para cada safeguard, documente: status (implementado, parcial, não implementado), evidência de implementação, data da última verificação, responsável. Esse registro é base para auditorias e demonstração de diligência.

Documente exceções e riscos aceitos. Quando a organização decide aceitar risco que você recomendou mitigar, registre formalmente. A decisão foi de quem tinha autoridade. Sua responsabilidade era informar, e você informou.

Guarde evidências de comunicação. E-mails alertando sobre riscos, apresentações para diretoria, atas de reuniões. Se você comunicou e não foi ouvido, a documentação demonstra que cumpriu seu papel.

Atualize periodicamente. Documentação desatualizada é quase tão ruim quanto ausência de documentação. Estabeleça cadência de revisão (trimestral é razoável) e cumpra.

Métricas que fazem sentido para executivos

Cobertura de inventário: percentual de ativos conhecidos versus estimativa de ativos totais. Meta é 100%, realidade frequentemente é menor. A lacuna indica risco.

Tempo médio para correção de vulnerabilidades críticas: quanto tempo entre descoberta de vulnerabilidade e aplicação de patch. Menos de 30 dias é razoável para críticas.

Percentual de implementação do IG1: quantos dos 56 safeguards estão implementados. Progresso trimestral demonstra evolução.

I ncidentes por período: quantos incidentes de segurança ocorreram, qual a severidade, qual o tempo de resposta. Tendência importa mais que número absoluto.

Custo por incidente: quando incidentes ocorrem, qual o custo de resposta e remediação. Justifica investimento em prevenção.

Para Advogados e Profissionais de Compliance

Seu papel é avaliar exposição e garantir que a organização possa demonstrar diligência. Você não precisa entender tecnologia. Precisa entender o que constitui cuidado razoável e como documentá-lo de forma defensável.

O que documentar para demonstrar diligência

Adoção formal de framework. Decisão documentada de que a organização adota CIS Controls como referência de segurança. Ata de reunião, política aprovada, ou comunicação formal servem como evidência.

Avaliação de maturidade. Relatório periódico indicando quais safeguards estão implementados, quais estão em progresso, quais não estão implementados e por quê. Demonstra consciência do estado atual.

Plano de evolução. Documento indicando como a organização pretende melhorar sua postura de segurança ao longo do tempo. Cronograma, responsáveis, recursos alocados. Demonstra intenção de melhoria contínua.

Registro de incidentes e respostas. Documentação de incidentes ocorridos, como foram detectados, como foram tratados, quais lições foram aprendidas. Demonstra capacidade de resposta.

Evidências de treinamento. Registros de que colaboradores receberam treinamento em segurança, quando, com qual conteúdo. Demonstra investimento em fator humano.

Como avaliar se a organização está exposta

Pergunte pelo IG1. Se a organização não implementou os 56 safeguards do baseline essencial, está exposta. A pergunta seguinte é: existe plano e cronograma para implementar?

Verifique a data das evidências. Inventário de ativos de 2022 não demonstra diligência em 2025. Política de segurança nunca revisada indica negligência. Evidências precisam ser atuais.

Avalie a qualidade das respostas. Quando você pergunta sobre determinado controle, a resposta é precisa ou vaga? Respostas precisas indicam controle real. Respostas vagas indicam teatro de compliance.

Teste a capacidade de resposta. Pergunte: se tivermos incidente amanhã, quem é acionado primeiro? Se a resposta for confusa ou demorar, o plano de resposta não está internalizado.

Relação entre CIS, LGPD e outras regulamentações

O capítulo 3 detalhou essa relação. A síntese para seu contexto: a LGPD exige "medidas técnicas e administrativas aptas a proteger os dados pessoais" (Art. 46). O CIS Controls oferece definição operacional do que essas medidas são. Implementar CIS é forma de demonstrar conformidade com a exigência legal.

O Controle 3 (Data Protection) endereça diretamente classificação e proteção de dados pessoais. O Controle 5 (Account Management) endereça controle de quem acessa dados. O Controle 8 (Audit Log Management) endereça capacidade de rastrear acessos. O Controle 17 (Incident Response) endereça capacidade de responder a incidentes de vazamento.

Para setores regulados, o CIS mapeia para frameworks específicos. Saúde pode correlacionar com requisitos de proteção de dados de saúde. Financeiro pode correlacionar com requisitos de reguladores bancários. Os mapeamentos disponíveis no site do CIS facilitam essa demonstração.

Preparação para fiscalizações e litígios

Organize evidências por controle. Quando auditor ou regulador perguntar sobre determinado aspecto, você deveria conseguir localizar evidência relevante rapidamente. Estrutura organizada demonstra maturidade.

Prepare narrativa de evolução. A pergunta do regulador pós-incidente não é apenas "o que vocês tinham?", mas "o que vocês estavam fazendo para melhorar?". Demonstrar trajetória de melhoria é tão importante quanto demonstrar estado atual.

Identifique lacunas antes que outros identifiquem. Autoavaliação honesta permite corrigir problemas antes que se tornem achados de auditoria ou argumentos de acusação. É melhor você descobrir a falha do que o regulador.

Documente contexto de decisões. Quando a organização decidiu não implementar determinado controle, qual era o contexto? Recursos limitados? Risco avaliado como baixo? Controle compensatório? Contexto transforma negligência aparente em decisão informada.

Para PMEs e Empresários

Você provavelmente acumula funções. É dono, é gestor, talvez seja também quem resolve problemas de TI. Recursos são limitados. Tempo é escasso. A tentação é ignorar segurança até que seja tarde demais.

Este livro existe em parte para você. O CIS Controls, especialmente o IG1, foi desenhado reconhecendo que nem toda organização tem departamento de TI, orçamento dedicado ou especialistas disponíveis.

O mínimo viável com recursos mínimos

Os 56 safeguards do IG1 parecem muito. Não são. Muitos são procedimentais, não técnicos. Muitos podem ser implementados com ferramentas gratuitas ou já incluídas em software que você usa. Muitos são práticas que você deveria ter independentemente de segurança.

Comece por três coisas.

Primeiro: saiba o que você tem. Liste todos os computadores, celulares, tablets, servidores, roteadores que sua empresa usa. Atualize essa lista quando algo muda. Isso é o Controle 1 em sua forma mais básica.

Segundo: proteja acessos. Senhas únicas e fortes para cada sistema. Autenticação de dois fatores onde disponível, especialmente email e sistemas financeiros. Revogue acesso de quem sai da empresa no mesmo dia. Isso cobre essência dos Controles 5 e 6.

Terceiro: tenha backup. Backup automático, em local diferente dos dados originais, testado periodicamente para confirmar que funciona. Quando ransomware chegar, e a questão é quando, backup é sua salvação. Isso é o Controle 11.

Esses três elementos, implementados com disciplina, cobrem os riscos mais prováveis e mais devastadores para PMEs.

O que terceirizar e o que manter interno

Terceirize infraestrutura quando possível. Usar e-mail em nuvem (Google Workspace, Microsoft 365) transfere responsabilidade de segurança do servidor de e-mail para provedor que tem mais recursos que você. Usar armazenamento em nuvem com backup automático é mais seguro que servidor local que ninguém mantém.

Mantenha interno o conhecimento. Mesmo que você terceirize TI para provedor de serviços, alguém na empresa precisa saber o que foi contratado, o que está sendo

feito, como verificar se está funcionando. Terceirizar execução não significa terceirizar responsabilidade.

Exija evidências de terceiros. Se você contratou empresa para "cuidar da segurança", pergunte: quais controles estão implementados? Qual o último relatório de status? Quando foi o último teste de backup? Terceiro que não consegue responder não está cuidando de nada.

Como "não fazer nada" é mais caro do que "fazer pouco"

O custo médio de incidente de segurança para PMEs frequentemente excede dezenas de milhares de reais. Inclui parada operacional, recuperação de dados, notificação de clientes, possíveis multas regulatórias, dano reputacional. Empresas pequenas fecham após incidentes graves porque não conseguem absorver o impacto.

Implementar IG1 com seriedade custa muito pequena fração disso. Muito pode ser feito com ferramentas gratuitas e tempo. O investimento é desproporcional ao risco evitado.

A matemática é simples. Se você não fizer nada e nada acontecer, você economizou esforço. Se você não fizer nada e algo acontecer, você pode perder a empresa. Se você fizer o básico e algo acontecer, você tem capacidade de responder e se recuperar.

O básico não garante que nada acontecerá. Garante que, quando acontecer, você não estará completamente desprotegido. E garante que, se precisar explicar a alguém, terá mais que negligência para mostrar.

O denominador comum

Independentemente do perfil, uma verdade atravessa todas as seções deste capítulo: *segurança é decisão, não tecnologia.*

O executivo decide priorizar ou ignorar. O gestor de TI decide implementar com rigor ou com displicência. O advogado decide exigir evidências ou aceitar respostas vagas. O empresário de PME decide investir tempo no básico ou torcer para que nada aconteça.

O CIS Controls oferece mapa. Implementation Groups oferecem priorização. Este livro oferece tradução. Mas nenhum framework, nenhuma ferramenta, nenhum consultor substitui a decisão de quem tem autoridade para agir.

O capítulo seguinte examina o que o CIS não resolve. Antes de chegar lá, é importante reconhecer que o CIS resolve muito, se houver decisão de implementá-lo. A limitação mais frequente não é do framework. É da vontade de usá-lo.

Referências do Capítulo

CENTER FOR INTERNET SECURITY. CIS Critical Security Controls Version 8.1. June 2024. Disponível em: https://www.cisecurity.org/controls/v8. Acesso em: jan. 2025.

CENTER FOR INTERNET SECURITY. Guide to Implementation Groups (IG): CIS Critical Security Controls v8.1. November 2024. Disponível em: https://www.cisecurity.org/controls/v8. Acesso em: jan. 2025.

CENTER FOR INTERNET SECURITY. CIS Controls Self Assessment Tool (CSAT). Disponível em: https://www.cisecurity.org/controls/cis-controls-self-assessment-tool-cis-csat. Acesso em: jan. 2025.

PONEMON INSTITUTE. Cost of a Data Breach Report 2024. IBM Security, 2024. Disponível em: https://www.ibm.com/reports/data-breach. Acesso em: jan. 2025.

NATIONAL CYBER SECURITY CENTRE (UK). Small Business Guide: Cyber Security. 2024. Disponível em: https://www.ncsc.gov.uk/collection/small-business-guide. Acesso em: jan. 2025.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: jan. 2025.

CAPÍTULO 9 - O que o CIS não resolve (e nunca prometeu)

O perigo da falsa completude

Frameworks bem construídos criam conforto. Checklists organizados transmitem sensação de controle. A tentação, depois de implementar 56 safeguards do IG1 ou mesmo os 153 do IG3, é acreditar que o trabalho está feito. Que a organização está "segura". Que riscos foram totalmente eliminados.

A tentação é armadilha.

O CIS Controls é framework poderoso, maduro, validado por décadas de experiência coletiva. Mas é framework, não solução total. Delimitar seus limites não é crítica ao CIS. É condição para usá-lo bem. Organizações que esperam do framework mais do que ele promete terminam frustradas ou, pior, expostas a riscos que imaginavam cobertos.

Este capítulo estabelece fronteiras. Não para diminuir o valor do CIS, mas para posicioná-lo corretamente no ecossistema de segurança corporativa. Saber o que o framework resolve é importante. Saber o que ele não resolve é igualmente crítico.

Engenharia social sofisticada

O CIS Controls aborda conscientização de segurança através do Controle 14, que estabelece programa de treinamento para força de trabalho. Os safeguards incluem treinamento para reconhecer ataques de engenharia social como phishing, pretexting e tailgating. É fundação necessária.

Mas fundação necessária não é defesa completa.

Engenharia social sofisticada opera em camada que treinamento padronizado não alcança. O atacante que passou semanas estudando o organograma da empresa, que conhece os nomes dos diretores, que sabe qual fornecedor está em negociação, que imita com precisão o estilo de comunicação do CEO, não será detectado por colaborador que aprendeu a desconfiar de e-mails com erros de português.

Business E-mail Compromise (BEC) avançado não depende de links maliciosos nem de anexos infectados. Depende de contexto, timing e conhecimento do alvo. O e-mail pode ser tecnicamente legítimo, vindo de conta comprometida de parceiro real, solicitando ação que faz sentido no contexto de negociação em andamento. Nenhum filtro técnico bloqueia. Nenhum treinamento genérico prepara.

O CIS fornece base. A defesa contra engenharia social sofisticada exige camadas adicionais: cultura organizacional que incentive verificação sem punir "paranoia", canais de confirmação fora do e-mail para transações sensíveis,

procedimentos que resistam mesmo quando atacante conhece o procedimento. Essas camadas estão além do escopo prescritivo do framework.

Ameaças internas maliciosas

O Controle 5 (Gestão de Contas) e o Controle 6 (Gestão de Controle de Acesso) estabelecem fundamentos para limitar o que cada pessoa pode fazer nos sistemas. Princípio do menor privilégio, segregação de funções, revisão periódica de acessos. São controles essenciais.

Mas controles de acesso presumem que o adversário está fora tentando entrar. Quando o adversário já está dentro, com acesso legítimo, os mesmos controles que protegem a organização protegem também a capacidade do “insider” de operar.

O funcionário descontente com acesso a dados financeiros não precisa explorar vulnerabilidade técnica. Precisa apenas de pen drive. O administrador de sistemas que decide sabotar a empresa antes de pedir demissão não precisa de ferramentas sofisticadas. Tem credenciais legítimas para fazer o estrago.

O CIS recomenda logging (Controle 8) e monitoramento (Controle 13), que podem ajudar a detectar comportamento anômalo. Mas detecção de insider malicioso é problema de análise comportamental que transcende a prescrição do framework. Exige correlação de eventos, estabelecimento de baselines individuais, capacidade de distinguir entre colaborador trabalhando legitimamente fora do horário e colaborador exfiltrando dados antes de sair da empresa.

Programas robustos de mitigação de ameaças internas integram segurança da informação com recursos humanos, jurídico e gestão de pessoas de formas que o CIS não pretende prescrever. O framework oferece peças do quebra-cabeça. A montagem completa requer componentes adicionais.

Ataques de estado-nação

Implementation Group 3 foi desenhado para organizações que precisam "abater ataques direcionados de adversários sofisticados e reduzir o impacto de ataques zero-day". A formulação é honesta: reduzir impacto, não eliminar ameaça.

Adversários estatais operam com recursos, paciência e sofisticação que excedem qualquer framework defensivo padronizado. Desenvolvem exploits para vulnerabilidades desconhecidas. Comprometem cadeias de suprimentos em pontos que a organização alvo sequer sabe que existem. Mantêm persistência por meses ou anos, adaptando técnicas cada vez que detectam investigação.

Organizações que são alvos primários de operações de inteligência estatal (infraestrutura crítica, defesa, diplomacia, pesquisa sensível) precisam de defesas que o CIS não pretende fornecer. Inteligência de ameaças específica ao setor. Análise forense contínua. Relacionamento com agências governamentais de defesa cibernética. Arquiteturas de segurança desenhadas sob premissa de que o adversário já está dentro.

O CIS eleva significativamente o nível para atacantes comuns. Contra operações estatais dedicadas, funciona como camada necessária mas insuficiente. Reconhecer essa limitação não é derrotismo. É calibração realista de expectativas.

Onde outros frameworks complementam

O CIS Controls não opera em vácuo. Posiciona-se deliberadamente como conjunto de ações específicas e mensuráveis que se integra a frameworks mais amplos de governança e gestão de risco.

O NIST Cybersecurity Framework (CSF) oferece estrutura estratégica de maturidade organizada em funções (Governar, Identificar, Proteger, Detectar, Responder, Recuperar) que orienta priorização e comunicação executiva. O CIS mapeia diretamente para o NIST CSF, fornecendo os "comos" específicos para os “os quês” estratégicos. Organizações que precisam de linguagem para o board e reguladores frequentemente usam NIST CSF como camada de comunicação sobre implementação CIS.

A ISO/IEC 27001 estabelece requisitos para sistemas de gestão de segurança da informação (SGSI) com caminho para certificação formal. O CIS não oferece certificação, não prescreve estrutura de gestão nem define requisitos de auditoria. Organizações que precisam de certificação reconhecida internacionalmente implementam 27001, frequentemente usando CIS como referência técnica para controles específicos.

O MITRE ATT&CK Framework (MITRE ATT&CK Framework, ou estrutura desenvolvida pela MITRE que cataloga o comportamento de adversários em ataques cibernéticos) cataloga táticas, técnicas e procedimentos (TTPs – Tactics, Techniques and Procedures) de adversários reais, oferecendo um vocabulário comum para descrever como ataques acontecem. O CIS Community Defense Model (CDM – Modelo de Defesa Comunitária do CIS) já integra o ATT&CK para demonstrar a eficácia dos controles contra técnicas específicas. Mas organizações com operações maduras de segurança usam o ATT&CK diretamente para threat hunting (caça a ameaças), purple teaming (colaboração entre equipes vermelha e azul para testar e aprimorar defesas) e avaliação contínua de capacidade defensiva (continuous defensive capability assessment).

O COBIT oferece framework de governança de TI que conecta tecnologia a objetivos de negócio, útil especialmente para organizações com requisitos formais de governança corporativa. O CIS não substitui COBIT; opera em camada diferente.

A relação entre frameworks não é competição. É especialização. O CIS faz muito bem o que se propõe a fazer: prescrever controles técnicos e processuais específicos e mensuráveis. O que não se propõe a fazer requer outros instrumentos.

Decisões que transcendem frameworks

Além de limitações técnicas e complementaridades com outros frameworks, existem dimensões de segurança que nenhum framework resolve porque não são problemas de controle. São problemas de decisão organizacional.

Cultura de segurança não se implementa por checklist. Organizações onde segurança é vista como obstáculo ao negócio, onde alertas são ignorados porque "sempre dá alarme falso", onde exceções viram regra porque "fulano precisa trabalhar", onde a pressão por resultados sempre prevalece sobre a disciplina de controles, essas organizações podem implementar todos os 153 safeguards e permanecer vulneráveis. O framework prescreve o que fazer. Não prescreve como fazer as pessoas quererem fazer.

Apetite a risco é decisão de negócio, não de segurança. Quanto a organização está disposta a investir para mitigar quais riscos é pergunta que executivos respondem, não frameworks. O CIS oferece base para essa conversa: se você implementar IG1, defenderá contra 74% das técnicas catalogadas no MITRE ATT&CK. Se implementar IG3, chegará a 86%. Mas a decisão de onde parar, quanto investir, quais riscos aceitar, é decisão de governança que transcende prescrição técnica.

Investimento em pessoas não aparece como safeguard específico, mas determina o sucesso de praticamente todos eles. Organizações que tratam segurança como projeto (implementar e encerrar) em vez de programa (operar e evoluir) descobrem que controles implementados degradam rapidamente. Configurações derivam. Inventários desatualizam. Processos caem em desuso. O CIS prescreve o que manter. Não prescreve como garantir recursos para manutenção contínua.

O CIS como ponto de partida

A mensagem deste capítulo pode parecer pessimista se lida isoladamente. Não é essa a intenção.

O CIS Controls resolve muito. Para a maioria das organizações, especialmente PMEs e empresas sem maturidade prévia em segurança, implementar IG1 representa

salto transformacional em postura defensiva. Os 56 safeguards do IG1 endereçam as causas raiz da maioria esmagadora dos incidentes documentados. Fazer bem o básico é a coisa mais impactante que a maioria das organizações pode fazer.

Mas fazer bem o básico não significa parar no básico. E não significa imaginar que o básico cobre tudo.

O CIS é ponto de partida, não destino final. É fundação sobre a qual outras capacidades se constroem. É linguagem comum que permite conversas produtivas entre técnicos, executivos, advogados e reguladores. É demonstração de diligência que posiciona a organização favoravelmente em fiscalizações e litígios.

O que o CIS não é: solução mágica, proteção absoluta, garantia de que nada acontecerá.

Organizações maduras entendem essa distinção. Implementam CIS como base. Complementam com outros frameworks conforme suas necessidades específicas. Desenvolvem capacidades que transcendem qualquer framework. E, fundamentalmente, tratam segurança como jornada contínua, não como projeto com data de término.

A honestidade como postura

Este capítulo pode parecer estranho em um livro que dedica centenas de páginas a defender a adoção do CIS Controls. Por que, no penúltimo capítulo, dedicar espaço a limitações?

A resposta está na premissa que orienta toda esta série: segurança efetiva requer honestidade intelectual.

Vender o CIS como solução completa seria desonestidade. Criaria expectativas irrealistas, geraria frustração quando limitações aparecessem, e, pior, poderia induzir organizações a negligenciar complementos necessários porque acreditam que "já fizeram o suficiente".

Posicionar o CIS corretamente, como framework poderoso com escopo definido, é condição para usá-lo bem. Organizações que entendem o que o CIS resolve e o que não resolve tomam decisões melhores sobre onde investir além do framework. Executivos que conhecem os limites fazem perguntas melhores. Profissionais de segurança que dominam as fronteiras constroem programas mais robustos.

A Conclusão que segue consolida a mensagem desta obra e a posiciona no contexto da série “High Security Invisible Core”. Antes de chegar lá, este capítulo estabelece verdade importante: o básico é muito. Mas o básico não é tudo. E saber a diferença é parte essencial da maturidade em segurança.

Referências do Capítulo

CENTER FOR INTERNET SECURITY. CIS Critical Security Controls Version 8.1. June 2024. Disponível em: https://www.cisecurity.org/controls/v8. Acesso em: jan. 2026.

CENTER FOR INTERNET SECURITY. CIS Community Defense Model v2.0. 2024. Disponível em: https://www.cisecurity.org/controls/v8. Acesso em: jan. 2026.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. Cybersecurity Framework Version 2.0. 2024. Disponível em: https://www.nist.gov/cyberframework. Acesso em: jan. 2026.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection. 2022. Disponível em: https://www.iso.org/standard/27001. Acesso em: jan. 2026.

MITRE CORPORATION. ATT&CK Framework. 2024. Disponível em: https://attack.mitre.org. Acesso em: jan. 2026.

ISACA. COBIT 2019 Framework. 2019. Disponível em: https://www.isaca.org/resources/cobit. Acesso em: jan. 2026.

VERIZON. 2024 Data Breach Investigations Report. 2024. Disponível em: https://www.verizon.com/business/resources/reports/dbir/. Acesso em: jan. 2026.

FBI. Internet Crime Complaint Center (IC3) Annual Report 2024. 2024. Disponível em: https://www.ic3.gov/. Acesso em: jan. 2026.

CONCLUSÃO - O Básico é Escolha, Não Ignorância

O fim da era do "não saber"

Durante décadas, executivos puderam alegar desconhecimento. Segurança da informação era domínio técnico, confinado a departamentos de TI, discutido em linguagem inacessível, tratado como custo operacional invisível até que algo desse errado. A ignorância, se não era virtude, pelo menos era desculpa plausível.

Essa era terminou.

O CIS Controls existe desde 2008, quando ainda se chamava SANS Top 20. A versão 8.1, consolidada e traduzida para dezenas de idiomas, está disponível gratuitamente. Implementation Groups segmentam recomendações por porte e maturidade. Guias de implementação detalham cada safeguard. Ferramentas de autoavaliação permitem diagnóstico sem custo. Mapeamentos conectam o framework a praticamente qualquer regulação ou padrão existente.

A informação está disponível. Os caminhos estão documentados. Os custos de entrada são mínimos. O que falta não é conhecimento. É decisão.

Organizações que em 2026 ainda operam sem controles básicos de segurança não o fazem por falta de orientação. Fazem por escolha, explícita ou implícita, de não priorizar o tema. E escolha, diferentemente de ignorância, carrega responsabilidade.

Decisão consciente de governança

Este livro foi escrito para transformar o CIS Controls de assunto técnico em instrumento de governança. A transformação importa porque governança implica responsabilidade, e responsabilidade implica consequência.

Quando um conselho de administração aprova orçamento que não contempla segurança básica, está tomando decisão de governança. Quando um CEO delega integralmente o tema para TI sem jamais perguntar sobre controles implementados, está tomando decisão de governança. Quando um diretor financeiro corta investimento em segurança para atingir meta trimestral, está tomando decisão de governança.

Nenhuma dessas decisões é técnica. Todas são escolhas sobre alocação de recursos, priorização de riscos, definição do que importa para a organização. E todas carregam implicações que transcendem o momento em que foram tomadas.

O CIS oferece referência objetiva para essas decisões. Implementation Group 1 define o mínimo. Os 56 safeguards não são sugestões vagas. São ações específicas, mensuráveis, implementáveis com recursos limitados. Decidir não

implementá-los é prerrogativa de quem governa. Mas é decisão que precisa ser consciente, documentada, assumida.

A pergunta que reguladores, auditores, seguradoras e tribunais farão após o incidente não é "vocês conheciam o CIS Controls?". É "conhecendo, o que vocês decidiram fazer?". A resposta a essa pergunta determina se a organização demonstra diligência ou negligência. E negligência, em ambiente regulatório cada vez mais rigoroso, tem preço.

O peso da responsabilidade pessoal

A Lei Geral de Proteção de Dados estabelece que controladores e operadores respondem por danos causados por violação da legislação. O Marco Civil da Internet atribui responsabilidades a provedores de aplicação. Legislação societária impõe deveres de diligência a administradores. Contratos com clientes e parceiros frequentemente incluem cláusulas de segurança com penalidades por descumprimento.

O ambiente jurídico brasileiro, acompanhando tendência global, caminha para responsabilização crescente de quem tinha poder de decisão e não agiu. A figura do "executivo que não sabia" perde credibilidade quando informação estava disponível e acessível. A defesa de "fizemos o possível" enfraquece quando o possível estava documentado em framework público e a organização escolheu não seguir.

Responsabilidade pessoal não é cenário hipotético. Multas administrativas da ANPD já atingem pessoas físicas além de pessoas jurídicas. Ações de responsabilidade civil contra administradores por falhas de governança ganham tração. Seguradoras incluem cláusulas de exclusão para incidentes decorrentes de negligência demonstrável.

O CIS Controls, nesse contexto, funciona como linha de defesa para quem decide. Implementar o framework não garante que nada acontecerá. Mas demonstra que a organização, e seus dirigentes, agiram com o cuidado que era razoável esperar. Na ausência do framework, a pergunta do regulador pós-incidente não tem resposta satisfatória.

Por que este livro é começo

InvisibleCore foi concebido como Volume Zero de uma arquitetura conceitual mais ampla. Estabelece fundamento operacional. Define o mínimo defensável. Traduz framework técnico para linguagem de governança. Mas não pretende esgotar o tema de segurança corporativa. Pretende criar base sobre a qual temas mais sofisticados podem ser desenvolvidos.

O CIS Controls endereça controles técnicos e processuais essenciais. Não endereça, nem pretende endereçar, a totalidade dos desafios que organizações enfrentam em ambiente digital hostil. Existem dimensões que exigem tratamento dedicado, capacidades que precisam ser construídas sobre a fundação que o CIS estabelece, horizontes que demandam preparação além do que qualquer framework de controles pode prescrever.

Os volumes seguintes desta série desenvolvem essas extensões.

A jornada que continua

O próximo volume, “Imunidade Digital”, desenvolve capacidade organizacional de detectar, responder e aprender com ameaças. Apresenta o ESC (Escritório de Segurança Corporativa) como estrutura de resposta que não gera custo fixo nem cria burocracia. Introduz o HIDS-BR (Human Intrusion Detection System) como framework que transforma colaboradores em sensores de segurança. Onde o CIS termina, Imunidade Digital começa: controles implementados precisam de pessoas que os operem, incidentes detectados precisam de estrutura que responda, lições aprendidas precisam de processo que as incorpore.

O terceiro volume, “Agentes Invisíveis’, enfrenta realidade que o CIS Controls não previu em sua concepção original: a proliferação de identidades não humanas. Contas de serviço, APIs, tokens, bots, agentes de inteligência artificial. Entidades que operam em nome de pessoas e organizações, com credenciais e permissões, mas sem rosto, sem crachá, sem responsabilização clara. O inventário de ativos do CIS é pré-requisito para mapear onde esses agentes operam. A gestão de acessos é fundação para governá-los. Mas governança completa de identidades não humanas exige extensões que o framework não oferece e que o terceiro volume desenvolve.

O quarto volume, “Ameaças Quânticas”, prepara organizações para horizonte que parece distante mas exige ação presente. Computadores quânticos capazes de quebrar criptografia atual ainda não existem em escala prática comercial. Mas dados criptografados hoje estão sendo capturados por adversários que aguardam pacientemente o momento de descriptografá-los. Preparação para esse cenário começa com inventário criptográfico, que deriva naturalmente do inventário de ativos do CIS. Classificação de dados sensíveis, gestão de provedores, governança de mudanças: todos elementos que dependem de controles básicos bem executados. Sem CIS implementado, crypto-agility é aspiração sem fundamento.

A sequência não é arbitrária. Cada volume constrói sobre o anterior. Pular etapas não acelera a jornada. Compromete a estrutura.

O convite desafiador

Este livro termina onde a jornada começa.

Se você é executivo ou conselheiro, o convite é para fazer as perguntas que este livro ensinou a fazer. Cobrar respostas. Exigir evidências. Tratar segurança como tema de governança, não como detalhe técnico delegável e esquecível.

Se você é gestor de TI ou segurança, o convite é para usar a linguagem que este livro oferece. Traduzir necessidades técnicas em termos que o alto escalão compreende. Documentar o que foi implementado e o que não foi. Proteger a organização e, não menos importante, proteger a si mesmo.

Se você é advogado ou profissional de compliance, o convite é para integrar o CIS às suas avaliações de risco e diligência. Reconhecer que "medidas técnicas e administrativas adequadas" tem referência objetiva. Usar o framework como critério, não como checklist decorativo.

Se você é empresário de PME, o convite é para começar. Não esperar ter recursos ideais. Não adiar até que pareça urgente. Implementar o que é possível com o que está disponível. Cinquenta e seis safeguards parecem muito até que se perceba que representam o mínimo, não o máximo.

O CIS Controls não é produto a ser comprado, certificação a ser obtida, projeto a ser concluído. É decisão a ser tomada e mantida. Decisão de que segurança importa. Decisão de que o básico será feito. Decisão de que negligência não é opção aceitável.

A decisão é sua.

E agora você não pode dizer que não sabia.

Referências da Conclusão

CENTER FOR INTERNET SECURITY. CIS Critical Security Controls Version 8.1. June 2024. Disponível em: https://www.cisecurity.org/controls/v8. Acesso em: jan. 2026.

CENTER FOR INTERNET SECURITY. Guide to Implementation Groups (IG): CIS Critical Security Controls v8.1. November 2024. Disponível em: https://www.cisecurity.org/controls/v8. Acesso em: jan. 2026.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: jan. 2026.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Marco Civil da Internet. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: jan. 2026.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Regulamento de Dosimetria e Aplicação de Sanções Administrativas. 2023. Disponível em: https://www.gov.br/anpd/pt-br. Acesso em: jan. 2026.

APÊNDICE A - Perguntas Essenciais para Avaliação de Postura

Orientação de uso

Este apêndice oferece roteiros de entrevistas estruturadas por perfil. O objetivo não é substituir avaliações técnicas formais, mas permitir que pessoas sem formação especializada identifiquem sinais de alerta e avaliem se a organização opera com diligência mínima.

As perguntas foram calibradas para o contexto de Implementation Group 1. Respostas negativas não indicam necessariamente falha grave, mas apontam áreas que merecem investigação adicional.

Para Executivos e Conselheiros

Perguntas a fazer ao responsável por TI ou segurança:

Sobre inventário e visibilidade

1. Temos lista atualizada de todos os equipamentos conectados à nossa rede, incluindo os que funcionários usam remotamente?
2. Sabemos quais softwares estão instalados em cada equipamento e se estão atualizados?
3. Conseguimos identificar em menos de 24 horas se um equipamento novo e não autorizado se conectou à rede?

Interpretação: Respostas negativas indicam que a organização não sabe o que tem. Sem saber o que tem, não há como proteger. Controles 1 e 2 do CIS não estão implementados.

Sobre proteção de dados

4. Sabemos onde estão armazenados os dados mais sensíveis da empresa (financeiros, pessoais de clientes, estratégicos)?
5. Esses dados estão criptografados, tanto nos servidores quanto nos laptops dos colaboradores?
6. Existe processo definido para descartar dados quando não são mais necessários?

Interpretação: Respostas negativas indicam exposição a vazamentos e descumprimento provável da LGPD. Controle 3 do CIS não está implementado.

Sobre acessos e contas

7. Cada pessoa tem credenciais individuais ou existem senhas compartilhadas?
8. Contas de funcionários que saíram da empresa são desativadas no mesmo dia da saída?
9. Pessoas com acesso administrativo aos sistemas usam contas separadas para tarefas do dia a dia?

Interpretação: Respostas negativas indicam que a organização não controla quem pode fazer o quê. Controles 5 e 6 do CIS não estão implementados.

Sobre preparação para incidentes

10. Se sofrermos ataque de ransomware hoje, temos backups que permitam recuperar operações em quanto tempo?
11. Existe pessoa designada para coordenar resposta a incidentes de segurança?
12. Sabemos quem precisamos notificar (ANPD, clientes, parceiros) em caso de vazamento de dados?

Interpretação: Respostas negativas indicam que a organização não está preparada para quando, não se, um incidente ocorrer. Controles 11 e 17 do CIS não estão implementados.

Sinais de alerta em respostas

- "Nosso fornecedor de TI cuida disso" sem evidência documental
- "Acho que sim" ou "provavelmente" para perguntas objetivas
- Incapacidade de responder sem consultar outras pessoas
- Respostas defensivas ou evasivas

Para Gestores de TI e Segurança

Perguntas para autoavaliação e preparação de reporte executivo:

Sobre documentação defensável

1. Consigo demonstrar, com evidências, quais controles de segurança estão implementados?
2. Existe registro formal das decisões sobre o que foi implementado e o que não foi, com justificativas?
3. Se um auditor pedir evidência de diligência amanhã, consigo fornecer em 48 horas?

Implicação: Documentação não é burocracia. É proteção para a organização e para os Gestores de TI e Segurança, pessoalmente.

Sobre comunicação com executivos

4. Consigo explicar nossos principais riscos de segurança em linguagem que o CEO entende?
5. Tenho métricas que demonstram evolução (ou deterioração) da postura de segurança ao longo do tempo?
6. Quando solicito recursos, apresento justificativa baseada em risco ou apenas em necessidade técnica?

Implicação: Segurança que não se comunica com o negócio não recebe recursos. Tradução é parte do trabalho.

Sobre priorização

7. Se tivesse que escolher apenas cinco controles para implementar com recursos atuais, saberia quais escolher e por quê?
8. Conheço o Implementation Group 1 do CIS e sei quais safeguards já implementamos e quais faltam?
9. Existe roadmap documentado de evolução da segurança, mesmo que simples?

Implicação: Fazer tudo é impossível. Priorizar sem critério é negligência disfarçada de pragmatismo.

Para Advogados e Profissionais de Compliance

Perguntas para avaliação de exposição:

Sobre diligência demonstrável

1. A organização adota algum framework reconhecido de segurança (CIS, ISO 27001, NIST)?
2. Existe documentação que comprove a implementação dos controles alegados?
3. A última avaliação de segurança foi realizada há menos de 12 meses?

Implicação jurídica: "Medidas técnicas e administrativas" do Art. 46 da LGPD implicitamente requer demonstração objetiva. Alegação sem evidência não constitui defesa.

Sobre preparação para incidentes

4. Existe plano de resposta a incidentes documentado e testado?

5. O plano contempla requisitos de notificação (ANPD, titulares, parceiros contratuais)?
6. Há registro de quem tem autoridade para tomar decisões durante crise?

Implicação jurídica: Prazo de 72 horas para comunicação à ANPD não permite improvisar. Ausência de plano é evidência de negligência.

Sobre responsabilidade pessoal

7. Administradores e conselheiros foram informados formalmente sobre riscos de segurança?
8. Decisões sobre investimento (ou não investimento) em segurança estão documentadas em ata?
9. Existe segregação clara entre responsabilidade técnica e responsabilidade de governança?

Implicação jurídica: Responsabilidade de administradores por falha de supervisão é tema consolidado. Documentação de ciência e decisão é proteção básica.

Para Empresários de PMEs

Perguntas de verificação rápida:

O mínimo vital (responda sim ou não)

1. Todos os computadores e celulares da empresa têm antivírus atualizado?
2. Usamos senhas diferentes para cada sistema importante?
3. Fazemos backup pelo menos semanal dos dados críticos?
4. Os backups ficam em lugar separado (nuvem ou local físico diferente)?
5. Já testamos se conseguimos restaurar um backup?
6. Sabemos quem tem acesso a que, nos nossos sistemas?
7. Quando alguém sai da empresa, removemos os acessos no mesmo dia?
8. Nossos colaboradores sabem reconhecer e-mail de phishing?
9. Temos alguém definido para chamar se houver problema de segurança?
10. Nosso contrato com o fornecedor de TI especifica responsabilidades de segurança?

Interpretação

- 8 a 10 respostas "sim": Base razoável. Documente o que faz e continue evoluindo.
- 5 a 7 respostas "sim": Exposição significativa. Priorize as lacunas identificadas.
- Menos de 5 respostas "sim": Risco elevado. Busque orientação profissional antes que incidente force a busca.

Realidade incômoda

Se você respondeu "não sei" a mais de três perguntas, o problema não é falta de controles. É falta de visibilidade. Você não sabe se está protegido ou exposto. Essa incerteza, por si só, é risco que precisa ser endereçado.

APÊNDICE B - Correlação CIS IG1 × LGPD × Seguros Cyber

Orientação de uso

Esta matriz identifica como os 56 safeguards do Implementation Group 1 se relacionam com requisitos da Lei Geral de Proteção de Dados e com controles tipicamente exigidos por seguradoras para subscrição de apólices cyber.

No cenário atual, o seguro cyber já funciona, na prática, como um barômetro de diligência mínima: seguradoras nacionais e internacionais condicionam a aceitação e a precificação das apólices à comprovação de controles preventivos concretos, como autenticação forte, criptografia, backups, gestão de vulnerabilidades e testes recorrentes. Longe de ser apenas um instrumento de transferência de risco financeiro, o seguro passou a operar como sinalizador de maturidade em segurança empresarial, indicando ao mercado e aos reguladores quais empresas efetivamente tratam o risco cibernético como prioridade e expondo, por contraste, aquelas que ainda não o fazem.

A correlação aqui, com a LGPD e Seguros Cyber não é exaustiva nem constitui parecer jurídico. Serve como ponto de partida para avaliação integrada de conformidade e para demonstrar que implementação do CIS IG1 endereça múltiplas obrigações simultaneamente.

Legenda

- LGPD: Indica artigo da Lei 13.709/2018 relacionado;
- Seguro: Indica se o controle é tipicamente exigido (E), frequentemente solicitado (F) ou ocasionalmente considerado (O) por seguradoras.

Os 18 Controles CIS IG1 aplicáveis

Controle 1: Inventário e Controle de Ativos Corporativos

Safeguard	Descrição resumida	LGPD	Seguro
1.1	Estabelecer e manter inventário detalhado de ativos	Art. 37 (registro de operações), Art. 46 (medidas técnicas)	E
1.2	Endereçar ativos não autorizados	Art. 46 (segurança)	F

Conexão LGPD: Inventário de ativos é pré-requisito para o registro de operações de tratamento exigido pelo Art. 37. Sem saber onde dados pessoais estão armazenados, o registro é necessariamente incompleto.

Conexão Seguros: Seguradoras avaliam se a organização tem visibilidade sobre seu ambiente. Ausência de inventário é indicador de imaturidade que afeta precificação ou elegibilidade.

Controle 2: Inventário e Controle de Ativos de Software

Safeguard	Descrição resumida	LGPD	Seguro
2.1	Estabelecer e manter inventário de software	Art. 46	F
2.2	Garantir que software autorizado seja suportado	Art. 46	E
2.3	Endereçar software não autorizado	Art. 46	F

Conexão LGPD: Software desatualizado ou não suportado frequentemente contém vulnerabilidades conhecidas. Operar com software vulnerável quando patches estão disponíveis dificulta alegação de "medidas adequadas".

Conexão Seguros: Uso de software sem suporte do fabricante é frequentemente cláusula de exclusão ou agravante em apólices cyber.

Controle 3: Proteção de Dados

Safeguard	Descrição resumida	LGPD	Seguro
3.1	Estabelecer e manter processo de gestão de dados	Art. 37, Art. 46, Art. 50	E
3.2	Estabelecer e manter inventário de dados	Art. 37	E
3.3	Configurar listas de controle de acesso a dados	Art. 46, Art. 47	E
3.4	Aplicar retenção de dados	Art. 15, Art. 16	F
3.5	Descartar dados de forma segura	Art. 16	F
3.6	Criptografar dados em dispositivos de usuário final	Art. 46	E

Conexão LGPD: Este controle é o mais diretamente relacionado à LGPD. Inventário de dados é base para registro de operações (Art. 37). Controle de acesso atende ao princípio da necessidade (Art. 6º, III). Retenção e descarte atendem aos Arts. 15 e 16. Criptografia é medida técnica explicitamente reconhecida.

Conexão Seguros: Criptografia de dados em repouso, especialmente em dispositivos móveis, é exigência praticamente universal para cobertura de vazamento de dados.

Controle 4: Configuração Segura de Ativos e Software

Safeguard	Descrição resumida	LGPD	Seguro
4.1	Estabelecer processo de configuração segura	Art. 46	F
4.2	Estabelecer processo de configuração segura para infraestrutura de rede	Art. 46	F
4.3	Configurar bloqueio automático de sessão	Art. 46	F
4.4	Implementar e gerenciar firewall em servidores	Art. 46	E
4.5	Implementar e gerenciar firewall em dispositivos de usuário	Art. 46	E
4.6	Gerenciar ativos e software de forma segura	Art. 46	F
4.7	Gerenciar contas padrão em ativos e software	Art. 46	E

Conexão LGPD: Configurações inseguras são vetor frequente de incidentes. Demonstrar processo de hardening é evidência de diligência técnica.

Conexão Seguros: Firewalls e gestão de contas padrão são controles básicos verificados em praticamente todas as avaliações de risco para subscrição.

Controle 5: Gestão de Contas

Safeguard	Descrição resumida	LGPD	Seguro
5.1	Estabelecer e manter inventário de contas	Art. 46, Art. 47	E
5.2	Usar senhas únicas	Art. 46	E
5.3	Desabilitar contas dormentes	Art. 46	E
5.4	Restringir privilégios administrativos a contas dedicadas	Art. 46, Art. 47	E

Conexão LGPD: Gestão de contas é fundamento do controle de acesso. O Art. 47 estabelece que agentes de tratamento devem adotar medidas para garantir que apenas pessoas autorizadas acessem dados pessoais.

Conexão Seguros: Controles de acesso são área de foco primário em avaliações de risco. Contas compartilhadas, senhas fracas e contas dormentes são indicadores de risco que afetam elegibilidade e preço.

Controle 6: Gestão de Controle de Acesso

Safeguard	Descrição resumida	LGPD	Seguro
6.1	Estabelecer processo de concessão de acesso	Art. 46, Art. 47	E
6.2	Estabelecer processo de revogação de acesso	Art. 46, Art. 47	E
6.3	Exigir MFA para aplicações expostas externamente	Art. 46	E
6.4	Exigir MFA para acesso remoto à rede	Art. 46	E
6.5	Exigir MFA para acesso administrativo	Art. 46	E

Conexão LGPD: Processos de concessão e revogação atendem ao princípio da necessidade. MFA é medida técnica reconhecida como adequada para proteção de acesso a dados pessoais.

Conexão Seguros: MFA é possivelmente o controle mais enfatizado por seguradoras em anos recentes. Ausência de MFA para acesso remoto e administrativo é frequentemente motivo de recusa de cobertura ou exclusão específica.

Controle 7: Gestão Contínua de Vulnerabilidades

Safeguard	Descrição resumida	LGPD	Seguro
7.1	Estabelecer processo de gestão de vulnerabilidades	Art. 46	E
7.2	Estabelecer processo de remediação	Art. 46	E
7.3	Executar gestão automatizada de patches de sistema operacional	Art. 46	E
7.4	Executar gestão automatizada de patches de aplicações	Art. 46	E

Conexão LGPD: Vulnerabilidades conhecidas não corrigidas são evidência de negligência. Processo documentado de gestão demonstra diligência contínua.

Conexão Seguros: Frequência e abrangência de patching são métricas avaliadas em subscrição. Sistemas desatualizados por mais de 30 dias frequentemente geram ressalvas ou exclusões.

Controle 8: Gestão de Logs de Auditoria

Safeguard	Descrição resumida	LGPD	Seguro
8.1	Estabelecer processo de gestão de logs	Art. 37, Art. 46	F
8.2	Coletar logs de auditoria	Art. 37, Art. 46	E
8.3	Garantir armazenamento adequado para logs	Art. 37	F

Conexão LGPD: Logs são evidência para demonstrar conformidade e para investigar incidentes. O registro de operações do Art. 37 se beneficia de logs técnicos que comprovem o que foi feito com dados pessoais.

Conexão Seguros: Capacidade de investigar incidentes afeta tanto a prevenção quanto a resposta. Seguradoras valorizam organizações que conseguem determinar escopo de vazamentos.

Controle 9: Proteções de E-mail e Navegador Web

Safeguard	Descrição resumida	LGPD	Seguro
9.1	Garantir uso apenas de navegadores e clientes de e-mail suportados	Art. 46	F
9.2	Usar serviços de filtragem DNS	Art. 46	F

Conexão LGPD: E-mail e navegador são vetores primários de ataque. Proteções reduzem probabilidade de incidente que resulte em vazamento.

Conexão Seguros: Proteções de e-mail (filtros anti-phishing, anti-malware) são verificadas em avaliações de risco, especialmente após crescimento de ataques BEC.

Controle 10: Defesas contra Malware

Safeguard	Descrição resumida	LGPD	Seguro
10.1	Implementar e manter software anti-malware	Art. 46	E
10.2	Configurar atualização automática de assinaturas anti-malware	Art. 46	E
10.3	Desabilitar execução automática para mídias removíveis	Art. 46	F

Conexão LGPD: Malware é causa frequente de vazamentos. Anti-malware atualizado é medida técnica básica esperada.

Conexão Seguros: Presença e atualização de anti-malware é controle verificado em praticamente todas as avaliações. Cobertura para ransomware frequentemente exige demonstração de defesas anti-malware.

Controle 11: Recuperação de Dados

Safeguard	Descrição resumida	LGPD	Seguro
11.1	Estabelecer e manter processo de recuperação de dados	Art. 46 (disponibilidade)	E
11.2	Executar backups automatizados	Art. 46	E
11.3	Proteger dados de recuperação	Art. 46	E
11.4	Estabelecer e manter instância isolada de dados de recuperação	Art. 46	E

Conexão LGPD: Disponibilidade é dimensão da segurança. Incapacidade de recuperar dados pessoais após incidente pode configurar violação.

Conexão Seguros: Backups são controle crítico para cobertura de ransomware. Seguradoras verificam frequência, teste de restauração e isolamento de backups (proteção contra criptografia por ransomware).

Controle 12: Gestão de Infraestrutura de Rede

Safeguard	Descrição resumida	LGPD	Seguro
12.1	Garantir que infraestrutura de rede esteja atualizada	Art. 46	F

Conexão LGPD: Infraestrutura de rede desatualizada pode conter vulnerabilidades que comprometam dados em trânsito.

Conexão Seguros: Avaliado como parte da postura geral de segurança, especialmente para organizações com infraestrutura complexa.

Controle 14: Conscientização e Treinamento de Segurança

Safeguard	Descrição resumida	LGPD	Seguro
14.1	Estabelecer e manter programa de conscientização	Art. 46, Art. 50	E
14.2	Treinar colaboradores para reconhecer engenharia social	Art. 46	E
14.3	Treinar colaboradores em melhores práticas de autenticação	Art. 46	E
14.4	Treinar colaboradores em melhores práticas de tratamento de dados	Art. 46, Art. 50	E
14.5	Treinar colaboradores sobre causas de exposição não intencional de dados	Art. 46	F
14.6	Treinar colaboradores para reconhecer e reportar incidentes	Art. 46, Art. 48	E
14.7	Treinar colaboradores sobre como identificar e reportar se ativos estão sem atualizações	Art. 46	O
14.8	Treinar colaboradores sobre perigos de redes inseguras	Art. 46	F

Conexão LGPD: O Art. 50 menciona explicitamente "ações educativas" como elemento de boas práticas de governança. Treinamento documenta esforço de conformidade.

Conexão Seguros: Treinamento de conscientização, especialmente simulações de phishing, é exigência frequente. Algumas apólices condicionam cobertura de BEC a programa de treinamento documentado.

Controle 15: Gestão de Provedores de Serviço

Safeguard	Descrição resumida	LGPD	Seguro
15.1	Estabelecer e manter inventário de provedores de serviço	Art. 37, Art. 39	F

Conexão LGPD: O Art. 39 estabelece que o operador deve realizar tratamento segundo instruções do controlador. Inventário de provedores é base para gestão de operadores e para demonstrar cadeia de responsabilidade.

Conexão Seguros: Dependência de terceiros é fator de risco avaliado. Organizações que não sabem quais provedores acessam seus dados têm perfil de risco elevado.

Controle 17: Gestão de Resposta a Incidentes

Safeguard	Descrição resumida	LGPD	Seguro
17.1	Designar pessoal para gerenciar tratamento de incidentes	Art. 48	E
17.2	Estabelecer e manter informações de contato para reporte de incidentes	Art. 48	E
17.3	Estabelecer e manter processo corporativo de reporte de incidentes (e-mail específico por exemplo)	Art. 48	E

Conexão LGPD: O Art. 48 exige comunicação de incidente de segurança à ANPD e ao titular em prazo razoável. Sem processo definido, cumprimento do prazo é improvável.

Conexão Seguros: Plano de resposta a incidentes é exigência comum. Algumas apólices incluem serviços de resposta a incidentes e exigem que segurado siga procedimentos definidos para acionar cobertura.

Síntese

A implementação completa do IG1 endereça:

- Todos os princípios de segurança do Art. 46 da LGPD (medidas técnicas e administrativas)
- Requisitos de registro do Art. 37
- Fundamentos para gestão de operadores conforme Art. 39
- Base para comunicação de incidentes conforme Art. 48
- Elementos de boas práticas de governança do Art. 50

Do ponto de vista de seguros cyber, o IG1 cobre a maioria dos controles tipicamente exigidos para elegibilidade básica. Controles de MFA, backup, anti-malware e gestão de patches são particularmente críticos para cobertura de ransomware, que representa parcela significativa dos sinistros atuais.

O controle 18 não se aplica ao IG1.

A correlação demonstra que investimento em CIS IG1 não é apenas medida de segurança. É investimento em conformidade regulatória e em segurabilidade.

APÊNDICE C - Glossário Executivo

Orientação de uso

Este glossário define termos que aparecem na obra em linguagem acessível a leitores sem formação técnica. Definições privilegiam compreensão prática sobre precisão acadêmica.

Ativo (Asset) Qualquer recurso de valor para a organização. No contexto de segurança, inclui equipamentos (computadores, servidores, celulares), software, dados e pessoas. "Inventário de ativos" significa saber o que você tem.

Autenticação multifator (MFA) Exigência de mais de uma forma de prova de identidade para acessar sistema. Tipicamente combina algo que você sabe (senha) com algo que você tem (celular para receber código) ou algo que você é (biometria). Dificulta acesso mesmo quando senha é comprometida.

Backup Cópia de segurança de dados armazenada separadamente do original. Permite recuperação em caso de perda, corrupção ou sequestro (ransomware). Backup só tem valor se testado regularmente.

CIS Controls Conjunto de 18 controles de segurança e 153 ações específicas preventivas (safeguards) desenvolvido pelo Center for Internet Security. Referência reconhecida internacionalmente para demonstrar diligência em segurança.

Criptografia Técnica que transforma dados legíveis em formato ilegível sem a chave correta. Protege dados mesmo que sejam acessados por pessoa não autorizada. "Criptografia em repouso" protege dados armazenados. "Criptografia em trânsito" protege dados sendo transmitidos.

Diligência (due diligence) Cuidado razoável que pessoa prudente exerceria nas mesmas circunstâncias. Em segurança, significa implementar controles proporcionais ao risco. Demonstrar diligência é defesa contra alegações de negligência.

Engenharia social Técnicas de manipulação psicológica para induzir pessoas a revelar informações ou executar ações. Inclui phishing (e-mails fraudulentos), pretexting (criação de cenários falsos) e tailgating (acesso físico por acompanhamento). Explora comportamento humano, não falhas técnicas.

Firewall Barreira que controla tráfego de rede entre zonas de confiança diferentes. Permite ou bloqueia conexões segundo regras definidas. Existe em versões de rede (protege perímetro) e de dispositivo (protege equipamento individual).

Framework Estrutura organizada de referência. Em segurança, conjunto de controles, processos e práticas que servem como guia para implementação. CIS Controls, NIST CSF e ISO 27001 são frameworks.

Implementation Group (IG) Classificação do CIS Controls que agrupa safeguards por nível de maturidade e recursos necessários. IG1 (56 safeguards) é o mínimo para qualquer organização. IG2 adiciona 74 safeguards. IG3 adiciona mais 23 para total de 153.

Incidente de segurança Evento que compromete ou pode comprometer confidencialidade, integridade ou disponibilidade de dados ou sistemas. Inclui desde tentativas de acesso não autorizado até vazamentos confirmados.

Inventário Lista completa e atualizada de itens. Inventário de ativos lista equipamentos e software. Inventário de dados lista onde dados sensíveis estão armazenados. Sem inventário, não há como saber o que proteger.

LGPD (Lei Geral de Proteção de Dados) Lei 13.709/2018 que regula tratamento de dados pessoais no Brasil. Estabelece direitos de titulares, obrigações de controladores e operadores, e sanções por descumprimento. Art. 46 exige "medidas de segurança, técnicas e administrativas".

Malware Software malicioso projetado para danificar, interromper ou obter acesso não autorizado a sistemas. Inclui vírus, trojans, ransomware e spyware. Anti-malware é software que detecta e bloqueia essas ameaças.

Patch Atualização de software que corrige falhas ou vulnerabilidades. "Gestão de patches" é processo de aplicar atualizações de forma sistemática e tempestiva. Sistemas sem patches recentes são alvos preferenciais de atacantes.

Phishing Tentativa de obter informações sensíveis (senhas, dados financeiros) através de comunicação fraudulenta que se passa por fonte confiável. Tipicamente via email, mas também por SMS, telefone ou redes sociais.

Privilégio Nível de permissão para executar ações em sistema. "Privilégio administrativo" permite alterações amplas. "Menor privilégio" é princípio de conceder apenas permissões necessárias para a função.

Ransomware Tipo de malware que criptografa dados da vítima e exige pagamento (resgate) para fornecer chave de descriptografia. Variantes modernas também roubam dados antes de criptografar, ameaçando divulgação (múltiplas- extorsões).

Safeguard No CIS Controls, ação específica e mensurável que implementa parte de um controle. Cada controle contém múltiplos safeguards. O termo enfatiza proteção, não apenas verificação.

Seguro cyber Apólice de seguro que cobre perdas decorrentes de incidentes de segurança. Pode incluir custos de resposta, notificação, recuperação, extorsão e responsabilidade civil. Cobertura e elegibilidade dependem de controles implementados.

Vulnerabilidade Fraqueza em sistema, processo ou comportamento que pode ser explorada para causar dano. Vulnerabilidades técnicas são falhas em software. Vulnerabilidades humanas são suscetibilidades a engenharia social.

Referências dos Apêndices

CENTER FOR INTERNET SECURITY. CIS Critical Security Controls Version 8.1. June 2024. Disponível em: https://www.cisecurity.org/controls/v8. Acesso em: jan. 2026.

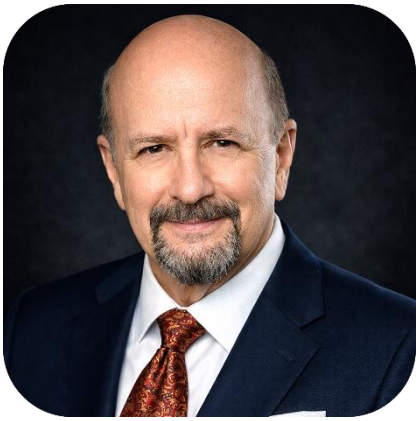
CENTER FOR INTERNET SECURITY. Guide to Implementation Groups (IG): CIS Critical Security Controls v8.1. November 2024. Disponível em: https://www.cisecurity.org/controls/v8. Acesso em: jan. 2026.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: jan. 2026.

MARSH. Cyber Insurance Market Overview 2024. Disponível em: https://www.marsh.com/. Acesso em: jan. 2026.

COALITION. Cyber Claims Report 2024. Disponível em: https://www.coalitioninc.com/. Acesso em: jan. 2026.

Sobre o Autor



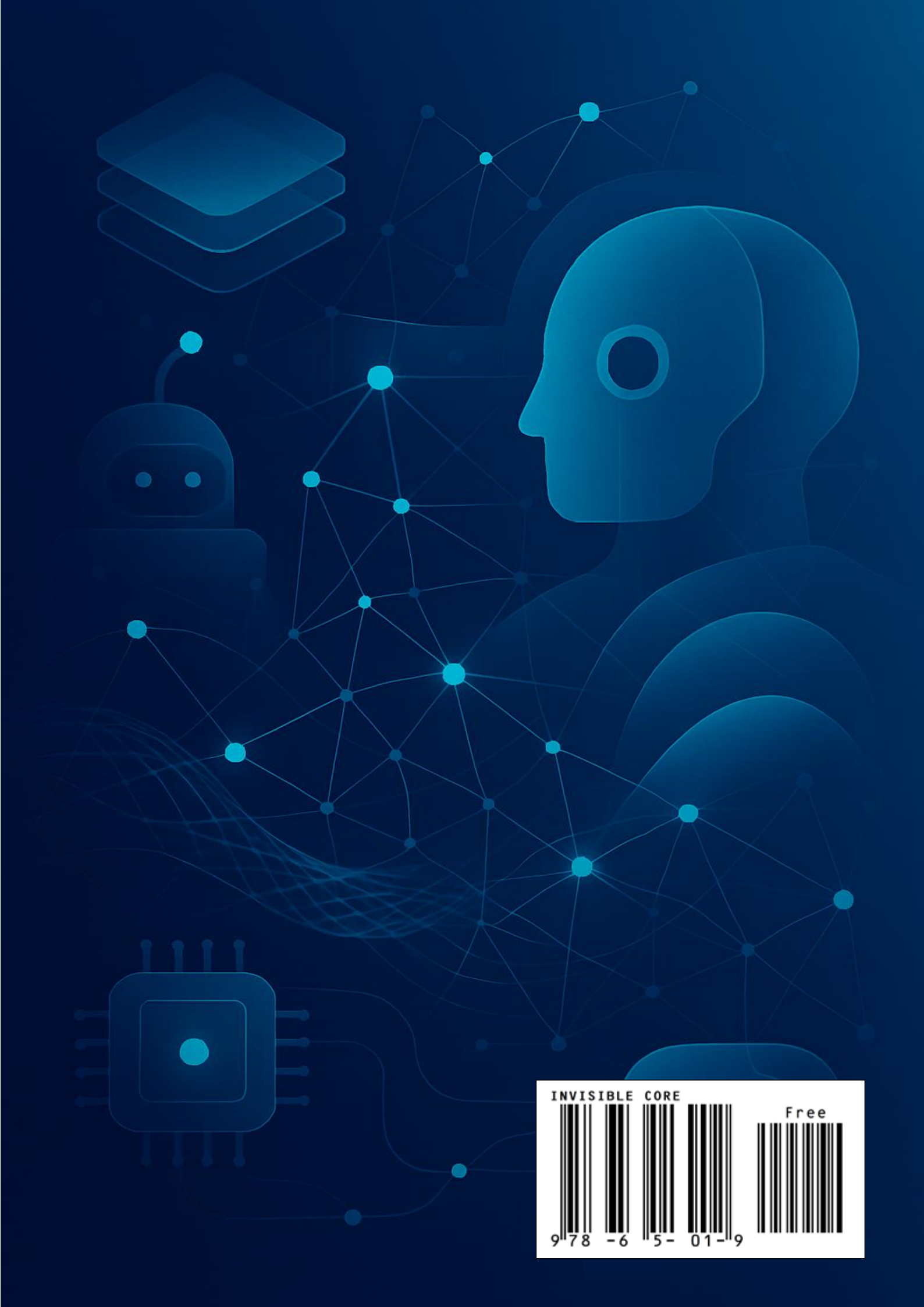
João Roberto Peres.

CEO - KSB Komp Security Brazil (30 anos) - Autor e Editor Internacional ISBN. Formação Engenheiro Eletricista, Administrador de Empresas, Mestre e Doutor em Ciências da Computação... Professor e Consultor da FGV (+20 anos) - Pesquisador multiespecialista em: Internet, IoT, AI, UI, UX, XR... Cybersecurity & Cybercrime, GRC / ESGT, Privacidade e Proteção de Dados - DPO, ISO/IEC 42001:2023, Metaverse & Cryptoactives, Open Innovation & Crowdsourcing, Foresight. Membro das Comissões: Privacidade Proteção de Dados e Inteligência Artificial - Direito Digital, da OAB-SP 2026 - Colaborador, Pesquisador e Autor no Projeto Internacional CyberSec4Europe – Obra: https://cybersec4europe.eu/wp-content/uploads/2023/02/The-Blue-Book.pdf

Mini-bio - Joao Roberto Peres – site migalhas – 2025 – disponível em: https://www.migalhas.com.br/autor/joao-roberto-peres - acesso em: 23/11/2025

Quadro Técnico da Obra

Objetivos:	Descrição:
Natureza	E-book técnico-profissional - Gratuito – licença **CC BY-NC**
Área	Segurança da Informação, Direito Digital, Governança – ZERO DA SÉRIE
Nível	Básico (acessível a não-especialistas)
Pré-requisitos	Nenhum conhecimento técnico prévio exigido
Público-alvo	Executivos, CISOs, DPOs, Advogados, Gestores de Risco, Técnicos SI
Abordagem	Prosa técnica referencial com orientação prática consultiva
Princípios Andragógicos	Técnicas diversas, em especial RRT (Repetition Reinforcement Technique)
Estrutura	Progressão linear com roteiros alternativos por perfil
Técnicas aplicadas	Analogias, casos de uso, checklists, templates, glossário comentado
Aplicabilidade	Imediata – questões prontas para uso organizacional
Extensão	~34.000 palavras
Tempo estimado de leitura	4-6 horas (integral)
Recursos complementares	Glossário simplificado
Apoio Plataforma WEB	Páginas de Apoio e atualização – tempo indeterminado sem previsão
Atualização	Conteúdo fechado em janeiro de 2026 – registro Janeiro de 2026.



INVISIBLE CORE

Free

9 78 -6 5- 01-9