REVISTA TÓPICOS
ISSN 2965-6672 | Qualis A2

FRAMEWORK DE GOVERNANÇA PARA O MONITORAMENTO PROPORCIONAL EM CENTROS DE OPERAÇÕES DE SEGURANÇA SOB A LGPD

A GOVERNANCE FRAMEWORK FOR PROPORTIONATE MONITORING IN SECURITY OPERATIONS CENTERS UNDER THE LGPD

Ciências Exatas e da Terra, Engenharias • 24/11/2026

REGISTRO DOI: 10.70773/revistatopicos/795427509

Daniel Monteiro de Carvalho[1]

Caio Cezar Jotta Nogueira[2]

Gabriel Victor Martins Carvalho[3]

Yago da Costa Jardim Alves Braga[4]

Christiane Martins de Vasconcellos Silveira[5]

Wellington Ávila[6]

RESUMO

O artigo analisa onde termina a segurança cibernética legítima e começa a vigilância exagerada de trabalhadores nos centros de operações de segurança (SOC), sob o olhar da Lei Geral de Proteção de Dados Pessoais (LGPD). O objetivo é identificar regras jurídicas e técnicas que façam o monitoramento ser justo e proporcional. A pesquisa, que é qualitativa, bibliográfica e documental, categorizou 120 fontes. Usando a abordagem *Design Science Research*, propõe um *framework* conceitual de governança dividido em seis etapas, acompanhado de um índice de prioridade e de uma modelagem de ameaças que combina STRIDE e LINDDUN. Em um cenário bancário hipotético, a avaliação *ex ante* recomendou suprimir o conteúdo das mensagens e da digitação em tempo real, agregar a geolocalização e pseudonimizar o identificador e o IP. O estudo conclui que segurança e proteção de dados podem convergir quando cada dado recolhido tem uma finalidade de defesa e uma base legal, e sugere testar em prova de conceito se a detecção contínua permanece eficaz depois dessas mudanças.

Palavras-chave: Segurança cibernética; Proteção de dados pessoais; LGPD; Vigilância no trabalho; Engenharia de privacidade.

ABSTRACT

This article examines the boundary between legitimate cybersecurity and disproportionate surveillance of workers in security operations centers (SOCs) under Brazil's General Data Protection Law (LGPD). It aims to identify legal and technical criteria that keep such monitoring proportionate. The qualitative, bibliographic and documentary research codes 120 sources and, drawing on Design Science Research, proposes a six-step conceptual governance framework supported by a heuristic prioritization index and by threat modeling that combines STRIDE and LINDDUN. In a

hypothetical banking scenario, the *ex ante* evaluation recommends removing message content and keystroke dynamics, aggregating geolocation and pseudonymizing user identifiers and IP addresses. The study concludes that security and data protection can converge when tool configuration ties each collected data element to a defensive purpose and a legal basis, and it proposes a proof of concept to test whether detection capability survives these transformations.
Keywords: Cybersecurity; Personal data protection; LGPD; Workplace surveillance; Privacy engineering.

1. INTRODUÇÃO

Os Centros de Operações de Segurança (*Security Operations Center,* SOC) operam 24 horas por dia, sete dias por semana. Eles correlacionam eventos dispersos em plataformas de *Security Information and Event Management* (SIEM), monitoram processos e conexões diretamente nas estações com agentes de *Endpoint Detection and Response* (EDR), inspecionam mensagens e arquivos para conter vazamentos (*Data Loss Prevention*, DLP) e modelam desvios comportamentais de contas e dispositivos (*User and Entity Behavior Analytics*, UEBA). Nenhuma dessas camadas funciona sozinha. Para distinguir ataques reais do tráfego ordinário, o sistema de segurança acaba por rastrear a rotina digital dos trabalhadores e por traçar perfis de seu comportamento.

Em uma definição adaptada do glossário federal, segurança cibernética se refere ao conjunto de ações que buscam fazer os sistemas de informação resistirem a eventos no espaço cibernético que comprometam disponibilidade, integridade, confidencialidade e autenticidade (Brasil, 2021). Entre julho de 2023 e junho de 2025, a

Agência Nacional de Proteção de Dados (ANPD)[7] registrou 723 comunicações de incidentes de segurança, entre os quais se destacaram o roubo de credenciais e a engenharia social (ANPD, 2025b).

Desde os primeiros estudos com pseudônimos em dados de auditoria (Biskup; Flegel, 2000) até arquiteturas modernas de SIEM moldadas ao Regulamento Geral sobre a Proteção de Dados europeu, o RGPD (Menges *et al.*, 2021), a engenharia de segurança busca conciliar detecção de intrusões e preservação da privacidade. No cenário brasileiro, iniciativas recentes já trataram partes específicas, como um guia para *logs* de autenticação em instituições federais de ensino superior (Cardoso; Gualberto, 2026) e um modelo de política de *logs* de auditoria para órgãos federais (Brasil, 2023b). Permanece aberta, contudo, uma lacuna estrutural: nenhum estudo localizado atravessa todo o *pipeline* de dados de um SOC, da coleta bruta na estação à reidentificação controlada do titular, amarrando cada etapa a hipóteses legais por cenário e às restrições próprias da relação de emprego. O tema ganhou relevância com a regulamentação da comunicação de incidentes e com a transformação da ANPD em agência reguladora (ANPD, 2024b; Brasil, 2026). No setor financeiro, pesaram também as novas exigências do Conselho Monetário Nacional (CMN) sobre segurança cibernética (Conselho Monetário Nacional, 2025).

No aspecto legal, o monitoramento de segurança deve se submeter à Lei Geral de Proteção de Dados Pessoais (LGPD, Lei nº 13.709/2018) e ao direito fundamental à proteção de dados previsto no art. 5º, inciso LXXIX, da Constituição Federal (CF). Nesse contexto, o presente artigo tem como objetivo geral entender quais critérios jurídicos e técnicos podem orientar a configuração de soluções de SOC, a fim

de conter o monitoramento de segurança dentro dos limites da proporcionalidade da LGPD. Para alcançá-lo, são definidos quatro objetivos específicos: (a) identificar as leis que regulam o monitoramento de segurança; (b) classificar as práticas que mais expõem os titulares; (c) elaborar e avaliar, de forma *ex ante*, um *framework* de governança; e (d) analisar os limites estruturais do modelo proposto.

O texto é direcionado a controladores, responsáveis pelo tratamento de dados, equipes de SOC e áreas jurídicas. Como contribuição, propõe-se um *framework* de governança que transfere ao monitoramento em centros de operações de segurança princípios e metodologias já existentes, como o *Privacy by Design*, o teste de balanceamento e as taxonomias de ameaças STRIDE e LINDDUN. Trata-se, na terminologia de Gregor e Hevner (2013), de uma exaptação. Para fins de organização, o artigo está estruturado da seguinte forma: a Seção 2 aborda o arcabouço legal; a Seção 3 descreve a metodologia; a Seção 4 classifica as práticas de exposição; a Seção 5 apresenta e avalia o *framework*; e a Seção 6 discute seus limites e conclusões.

2. FUNDAMENTAÇÃO TEÓRICA E NORMATIVA

2.1. Da Privacidade à Proteção de Dados Pessoais

Registrada por Cooley (1888) e difundida por Warren e Brandeis (1890), a expressão *right to be let alone* concebia a privacidade como direito de afastar a intromissão de terceiros, especialmente diante da imprensa e da fotografia instantânea. Quando o processamento automatizado surgiu, tornou insuficiente essa ideia negativa. Ao julgar a lei do recenseamento, em 1983, o Tribunal Constitucional

Federal alemão reconheceu a autodeterminação informativa, o poder de cada pessoa decidir sobre a divulgação e o uso de seus dados. O tribunal também advertiu que, quando há tratamento automatizado, não existe dado insignificante (Alemanha, 1983). Rodotà (2008) interpreta essa passagem como deslocamento do sigilo para o controle sobre a circulação da informação. Doneda (2019) utiliza a mesma interpretação para sustentar a autonomia da proteção de dados no direito brasileiro.

Críticas posteriores atingiram o próprio modelo do controle individual, trazendo reflexos diretos sobre o SOC. Para Nissenbaum (2004), a privacidade é violada quando um fluxo de informação rompe as normas do contexto em que ocorreu, borrando a fronteira tradicional entre dado público e privado. No ambiente de trabalho, essa diferença é decisiva. Como o controle individual pouco protege nesse cenário, a telemetria coletada para detectar intrusões ilustra bem o ponto: ela respeita as regras do contexto de segurança, mas as viola frontalmente caso venha a alimentar avaliações de desempenho do funcionário. Solove (2006) segue uma linha semelhante, ao evidenciar que o processamento posterior à coleta gera danos próprios, como a agregação de registros individualmente inofensivos e o uso secundário desses dados. Em obra posterior, ele rejeitou a oposição entre privacidade e segurança como um falso dilema e sugeriu discutir a supervisão das medidas de segurança (Solove, 2011).

No Brasil, essa trajetória chegou à Constituição graças à Ação Direta de Inconstitucionalidade 6.387/DF, em que o Supremo Tribunal Federal (STF) suspendeu o compartilhamento de dados de usuários de telefonia com o Instituto Brasileiro de Geografia e Estatística (IBGE). Ao fazer isso, o tribunal reconheceu a proteção de dados

como direito fundamental autônomo, seguindo a decisão alemã (Brasil, 2020; Mendes; Rodrigues Júnior; Fonseca, 2021). A Emenda Constitucional nº 115/2022 positivou esse direito no art. 5º, LXXIX, e atribuiu à União a competência exclusiva para criar leis sobre o assunto (Brasil, 2022; Acioly; Silva; Monteiro Neto, 2024).

2.2. Segurança da Informação, Engenharia de Privacidade e Estudos Próximos

Nas normas técnicas, a segurança da informação abrange confidencialidade, integridade, disponibilidade, autenticidade, responsabilização e não repúdio (ISO, 2018; ABNT, 2022a, 2022b). No *National Institute of Standards and Technology* (NIST), a resposta a incidentes passou do ciclo de quatro fases (Cichonski *et al.*, 2012) à integração com o *Cybersecurity Framework* (CSF) 2.0 (NIST, 2024; Nelson *et al.*, 2025), apoiada em telemetria com prazos definidos de retenção e descarte (Kent; Souppaya, 2006). Em privacidade, existem referenciais de gestão, como a ISO/IEC 27701, autônoma desde 2025 (ABNT, 2019; ISO, 2025), e o NIST *Privacy Framework* (NIST, 2020), além da engenharia de privacidade (Spiekermann; Cranor, 2009; Hoepman, 2014). Os estudos mais recentes tratam de *pipelines* de anonimização orientados à LGPD (Resende; Portes Filho; Santos Filho, 2026), de detecção de intrusão por aprendizado federado (Hernandez-Ramos *et al.*, 2025) e de extensão do LINDDUN à autenticação (Robles-González; Parra-Arnau; Forné, 2020). Cada um cobre apenas parte do problema. A comparação feita no Apêndice C mostra que nenhum deles reúne o *pipeline* completo do SOC, a ancoragem na LGPD por dispositivo, as hipóteses legais por cenário e a relação de emprego.

2.3. A LGPD Aplicada à Segurança Cibernética

Sob a LGPD, o monitoramento subordina-se aos princípios do art. 6º (Brasil, 2018) e requer uma hipótese legal para cada operação, como a coleta de *logs* de autenticação ou a análise comportamental (Quadro 1). A obrigação legal ou regulatória (art. 7º, II) limita-se ao que a norma efetivamente impõe. O dever de segurança do art. 46, cujo descumprimento gera responsabilidade (art. 44, parágrafo único), demanda medidas capazes de proteger os dados, mas não especifica quais tratamentos as justificam. Parte-se da premissa de que esse dever ampara, no máximo, o registro indispensável à proteção; logo, a análise comportamental contínua exige outra hipótese legal.

Quanto ao exercício regular de direitos (art. 7º, VI), a letra da lei restringe o exercício a processos judiciais, administrativos ou arbitrais. Adota-se aqui a leitura restritiva: a hipótese apoia a preservação de evidências quando há um incidente concreto apto a gerar processo, mas não justifica a retenção forense puramente preventiva. A distinção não é meramente teórica. Usar a ampla defesa constitucional (CF, art. 5º, LV) para armazenar telemetria por prazo indeterminado, sem fato gerador definido, violaria por completo o princípio da necessidade (art. 6º, III). Órgãos públicos, por sua vez, vinculam o tratamento às competências legais (art. 23), com hipótese no art. 7º, II ou III. Fora de regras como dever regulatório, resposta a incidentes e competências públicas, o monitoramento cotidiano recai, em regra, no legítimo interesse (art. 7º, IX), já que o consentimento (art. 5º, XII) raramente é livre no emprego, devido à assimetria entre as partes (Article 29 Data Protection Working Party, 2017; Bioni, 2019).

Quadro 1. Hipóteses legais possíveis por cenário de monitoramento

Cenário e operação	Hipótese legal possível	Condições e salvaguardas
Trilhas de auditoria e detecção de intrusão em instituição autorizada pelo Banco Central do Brasil (BCB).	Obrigação regulatória (art. 7º, II), nos limites do art. 3º, §§ 2º e 7º, da Res. CMN nº 4.893/2021 ou da Res. BCB nº 85/2021.	Restrita ao que a norma exige, com retenção por tipo de processamento. A análise comportamental exige outra hipótese.
SIEM e EDR em ativos corporativos de organização não regulada.	Legítimo interesse (arts. 7º, IX, e 10), por operação.	Teste de balanceamento, minimização e transparência, com RIPD em alto risco. Inaplicável a dados sensíveis.
UEBA do empregador em equipamento corporativo.	Legítimo interesse, pois o consentimento raramente é livre no emprego.	Aviso prévio, canal de contestação, revisão humana e vedação do uso disciplinar direto dos alertas.
DLP do empregador em mensagens.	Legítimo interesse, conforme o canal.	Na conta corporativa, padrões classificados, com aviso. Na conta pessoal, bloqueio ou registro apenas de metadados. Em equipamento pessoal, coleta limitada ao ambiente corporativo.
Teletrabalho ou dispositivo pessoal com EDR.	Legítimo interesse, restrito ao ambiente corporativo.	Contêiner isolado e escopo em contrato escrito, que não substitui o teste de balanceamento.
Monitoramento da própria rede por órgão público.	Competências legais (art. 23), com base no art. 7º, II ou III.	Vinculação à finalidade pública e publicidade do tratamento.

Preservação de evidências na resposta a incidente.	Exercício regular de direitos (art. 7°, VI), se apto a gerar processo (tese restritiva adotada).	Preservação seletiva e cadeia de custódia (ABNT, 2013).

Fonte: Elaborado pelos autores (2026), com base em Brasil (2018), Conselho Monetário Nacional (2021, 2025), Banco Central do Brasil (2021) e ANPD (2024a). A hipótese aplicável depende da análise concreta de cada operação.

Quatro requisitos condicionam o legítimo interesse: finalidade legítima, dados estritamente necessários, transparência e respeito às legítimas expectativas do titular (art. 10). Seu cumprimento é aferido pelo teste de balanceamento que a ANPD orienta, inaplicável a dados sensíveis (ANPD, 2024a).

Em contraste com o RGPD, cujo Considerando 49 reconhece expressamente a segurança de redes como interesse legítimo (União Europeia, 2016a), a LGPD não possui previsão equivalente. O desafio jurídico se agrava quando o monitoramento atinge dados sensíveis. Para esses dados, o art. 11, II, g, prevê a prevenção à fraude nos processos de identificação e autenticação "de cadastro" (Brasil, 2018). Uma leitura ampla incluiria a autenticação contínua durante a sessão. A escolha recai sobre a leitura restritiva, que encontra respaldo no próprio texto ao vincular a autenticação ao cadastro. A doutrina e a regulação ainda não resolveram a questão. Em 2025, a ANPD realizou uma consulta sobre dados biométricos e consolidou as contribuições em nota técnica, com a ressalva de que o procedimento não representa seu posicionamento final (ANPD, 2025c; Brasscom, 2025).

Embora a LGPD qualifique o dado biométrico como sensível (art. 5º, II), o legislador não definiu um conceito claro. Sinais comportamentais, como a dinâmica de digitação, figuram entre as técnicas biométricas descritas pelas autoridades europeias (Article 29 Data Protection Working Party, 2012), mas o enquadramento jurídico não é automático, a exemplo do RGPD (União Europeia, 2016a, art. 4º, ponto 14). Tudo gira em torno da finalidade e da técnica de tratamento empregadas. Por isso, recorre-se a um teste funcional, semelhante aos requisitos defendidos pelo setor de tecnologia na mesma tomada de subsídios (Brasscom, 2025), no qual o sinal é biométrico quando tratado para reconhecer ou distinguir univocamente uma pessoa. Métricas de uso, como a contagem de teclas, não atendem a esse requisito. Quando o sinal é biométrico, cabe demonstrar que o tratamento é indispensável e que não há meio menos invasivo (Carneiro, 2026).

No plano arquitetônico, o art. 46, § 2º, exige que as medidas de segurança sejam observadas desde a concepção do produto ou do serviço. Não se deve confundir esse dever preventivo com os prazos do regulamento de incidentes (ANPD, 2024b), que fixa três dias úteis para a comunicação e cinco anos para o registro de todo incidente, sem autorizar que a telemetria bruta seja retida pelo mesmo período. O Relatório de Impacto à Proteção de Dados Pessoais (RIPD) é exigido (arts. 10, § 3º, e 38) e recomendado em alto risco (ANPD, 2023b), aferido pelo art. 4º da Resolução CD/ANPD nº 2/2022 (ANPD, 2022).

No campo das decisões unicamente automatizadas, o art. 20 assegura a revisão. Porém, não exige que ela seja feita por pessoa natural, pois a regra que impunha essa condição foi anulada (Brasil, 2019). Como um escore que se limita a orientar a triagem não se

considera uma decisão automatizada segundo o artigo, a revisão humana passa a ser salvaguarda recomendada (*cf.* Wachter; Mittelstadt; Floridi, 2017), cujo sucesso depende da capacidade do analista de resistir ao viés da automação (Parasuraman; Manzey, 2010). Se o escore, sozinho, bloquear contas ou impor sanções, o titular tem direito a solicitar revisão e a saber os critérios usados, ressalvados os segredos comerciais e industriais (art. 20, §§ 1º e 2º). Por fim, os direitos dos titulares elencados no art. 18 aplicam-se integralmente ao contexto do SOC. Vale ressaltar que a exclusão da LGPD prevista no art. 4º, III (voltada à segurança pública e persecução penal), não abrange investigações corporativas internas. Tais investigações permanecem sujeitas à lei, sendo amparadas pelo exercício regular de direitos (art. 7º, VI) e devendo observar rigorosamente as normas técnicas de cadeia de custódia (ABNT, 2013).

2.4. Legislação Correlata e Regulação Setorial

O Marco Civil da Internet obriga os provedores de conexão a guardar registros de um ano, e os provedores de aplicações a guardar registros de seis meses (Brasil, 2014, arts. 13 e 15), sem alcançar a telemetria interna de outras organizações. Quanto à inspeção de conteúdo pelo DLP, o sigilo das comunicações (Brasil, 1988, art. 5º, XII) impõe barreiras diretas. Embora o Tribunal Superior do Trabalho (TST) tenha admitido o controle formal e material do *e-mail* corporativo, separado do pessoal (Brasil, 2005), a LGPD exige que essa prática atenda aos requisitos de necessidade e transparência (Ico, 2023). O direito do trabalho segue a mesma lógica. A doutrina trabalhista sustenta que o poder diretivo (art. 2º da Consolidação das Leis do Trabalho, a CLT) não se aplica à vida privada do empregado (Oliveira Neto, 2023; Oliveira; Silva, 2024), e o contrato de teletrabalho

(arts. 75-C e 75-D da CLT) também não autoriza, por si só, a vigilância de atividades privadas (Brasil, 1943).

No setor financeiro, existem regras específicas. A Resolução CMN nº 4.893/2021 obriga, no art. 3º, § 2º, autenticação, criptografia, detecção de intrusão, prevenção de vazamento e rastreabilidade. O § 7º, inserido pela Resolução CMN nº 5.274/2025, trata das trilhas de auditoria, retidas por tempo definido pela instituição (Conselho Monetário Nacional, 2021, 2025). Para as instituições de pagamento, o Banco Central do Brasil (BCB) publicou regras análogas (Banco Central do Brasil, 2021, 2025). Como obrigação regulatória, essas normas cobrem apenas os controles listados. Qualquer atividade além desse escopo, como a análise comportamental, depende de outra hipótese legal. A Política Nacional de Cibersegurança orienta a matéria (Brasil, 2023a). Também há projetos de lei sobre inteligência artificial (IA) e segurança cibernética (Brasil, 2023c, 2025), em paralelo à regulação europeia da IA (União Europeia, 2024, 2026).[8]

3. METODOLOGIA

3.1. Seleção e Análise das Fontes

De natureza teórico-aplicada, o estudo combina abordagem qualitativa e finalidade exploratória a partir de fontes bibliográficas e documentais (Gil, 2017). Optou-se pela revisão narrativa por duas razões de ordem prática. Primeiro, porque atos normativos, decisões administrativas e judiciais e normas técnicas da ISO e do NIST escapam à indexação das bases científicas tradicionais. Segundo, porque Direito e Ciência da Computação usam jargões que raramente convergem em uma *string* booleana única. A própria arquitetura do artefato exigiu esse desenho, pois cada decisão

técnica do *pipeline* tinha que se basear diretamente em um dispositivo legal ou em uma norma técnica. A seleção foi intencional e combinou repositórios oficiais, buscas no Google Scholar e em portais de editores, com termos em português e inglês, e rastreamento de citações, até a data de corte de 3 de novembro de 2026. Ficaram de fora materiais promocionais e textos sem lastro normativo ou empírico. O desenho tem um custo. Como o número de resultados brutos de cada busca não foi registrado, a seleção não pode ser reproduzida com exatidão, o que reduz a força das conclusões da revisão. O Quadro 5 do Apêndice A descreve o protocolo seguido e o registro a adotar nas atualizações, e o Quadro 6 apresenta o livro de códigos. O *corpus* final reúne 120 fontes, das quais 33 são artigos em periódicos revisados por pares. Em todo o artigo, normas e decisões estrangeiras servem apenas como parâmetro comparativo e interpretativo, sem força vinculante no Brasil. Usando o critério de suficiência analítica, o levantamento foi dado por concluído quando todas as categorias do livro de códigos, os sete cenários do Quadro 1 e os cinco elementos do *pipeline*, passaram a encontrar suporte em ao menos uma fonte primária.

Na análise documental (Bowen, 2009), adotou-se codificação temática dedutiva, com categorias prévias extraídas dos princípios do art. 6º e dos parâmetros do regulamento de dosimetria da LGPD. Outras categorias vieram de duas taxonomias complementares de ameaças: a STRIDE, voltada à segurança (Shostack, 2014), e a LINDDUN, voltada à privacidade (Deng *et al.*, 2011; Sion *et al.*, 2025). Ambas foram aplicadas a cada elemento do *pipeline* do SOC: da fonte à reidentificação, passando pela ingestão, pelo armazenamento e pela consulta. Em seguida, cada cruzamento foi classificado pelo efeito que o controle de segurança exerce sobre a ameaça à privacidade. Três resultados eram possíveis. O primeiro é

de convergência, quando o controle reduz a ameaça à privacidade. O segundo é de tensão, que ocorre se o controle de segurança aumenta a ameaça, mas existe uma medida compensatória de conciliação capaz de satisfazer ambos os objetivos. O terceiro, por fim, é o conflito, configurado quando nenhum controle examinado atende aos dois objetivos no mesmo escopo. A codificação foi realizada por um único pesquisador, sem o cálculo de medidas de confiabilidade interavaliadores. Para mitigar essa limitação, o livro de códigos e a matriz detalhada (Apêndice E) foram estruturados de modo a permitir que terceiros auditem ou repliquem cada classificação. Além disso, a recodificação independente de uma amostra está prevista na agenda de trabalhos futuros para validação do estudo.

3.2. Construção e Procedimento de Avaliação do Artefato

Por se tratar do esforço de converter normas e princípios jurídicos em decisões técnicas verificáveis, a construção do *framework* baseia-se na *Design Science Research* (DSR), conforme as diretrizes de Hevner *et al.* (2004). O processo de desenvolvimento segue as atividades propostas por Peffers *et al.* (2007) e fundamenta-se em seis requisitos principais: a ancoragem normativa (R1), o artefato verificável por passo (R2), a aplicabilidade ao contexto de SOC (R3), a explicitação de *trade-offs* (R4), a proporcionalidade ao porte da organização (R5) e a compatibilidade com referenciais consolidados (R6). O cumprimento de cada requisito pode ser verificado no próprio artefato. O R1, por exemplo, só é atendido se cada passo indicar expressamente os dispositivos da LGPD que o regem (Quadro 15). Essa avaliação, classificada como formativa e *ex ante* (Venable; Pries-Heje; Baskerville, 2016), teve o propósito de refinar o artefato antes de sua efetiva implementação. O método combinou a

formulação de argumentos lógicos fundamentados à simulação de aplicação em dois cenários hipotéticos: o de uma instituição bancária e o de uma pequena empresa. Cabe destacar que o modelo ainda não foi empregado por nenhuma organização real. Nos resultados, um requisito é classificado como "atendido" quando a evidência repousa integralmente no próprio desenho do artefato; "atendido no desenho" quando sua comprovação definitiva depender do uso real no campo; ou "atendido parcialmente" nos demais cenários de incerteza. O *framework* assume, portanto, o estatuto de uma proposta conceitual robusta, visto que esta primeira avaliação prescinde de painéis de especialistas e não aferiu sua eficácia empírica no ambiente de produção.

Como o estudo usa somente fontes bibliográficas e documentais de acesso público e cenários hipotéticos, sem participantes humanos, enquadra-se nas hipóteses de dispensa de registro e avaliação pelo sistema dos Comitês de Ética em Pesquisa e da Comissão Nacional de Ética em Pesquisa (CEP/Conep) previstas no art. 1º, parágrafo único, II, III e VI, da Resolução nº 510/2016 do Conselho Nacional de Saúde (Brasil, 2016). As fontes analisadas estão listadas nas referências, e as normas técnicas e parte dos livros são de acesso pago. A matriz STRIDE + LINDDUN e a planilha do *corpus* serão depositadas em repositório aberto após a publicação. Os autores declaram não haver conflito de interesses. Não houve financiamento específico.

4. CONFLITOS ENTRE SEGURANÇA CIBERNÉTICA E PRIVACIDADE

4.1. Tensões Centrais

As quatro ferramentas descritas na Introdução tratam dados pessoais, já que até endereços de protocolo de internet (IP) dinâmicos o são considerados dados pessoais quando associáveis a alguém (União Europeia, 2016b). O tempo de armazenamento é o primeiro ponto de tensão, pois manter *logs* por prazo indefinido vai contra a necessidade e a limitação da conservação (art. 6º, III, e arts. 15 e 16), além de transformar os bancos de dados em alvos de alto valor. A preservação forense deve se manter dentro dos limites do incidente.

Quanto mais amplo o escopo da coleta, maiores os riscos à privacidade. Instalado em equipamentos de *home office* ou do próprio computador do empregado, o EDR leva a coleta à vida privada e a dados de familiares (Ajunwa; Crawford; Schultz, 2017). DLP e EDR captam também, incidentalmente, dados de quem nem sequer faz parte do quadro de pessoal, como clientes e candidatos a vagas. No caso *Bărbulescu*, a Corte Europeia de Direitos Humanos listou como fatores a considerar, antes de monitorar as comunicações de um empregado, o aviso prévio, a extensão do monitoramento, a existência de razões legítimas, a disponibilidade de meios menos invasivos, as consequências para o empregado e as medidas de proteção adotadas (Conselho da Europa, 2017), critérios que o *framework* incorpora aos Passos 2 e 5.

Quando opacos, os escores do UEBA também podem discriminar (Mendes; Mattiuzzo, 2019). O risco aumenta porque ameaças internas são raras e os dados de treinamento são desequilibrados (Al-Shehari *et al.*, 2024). Com eventos tão raros, até detectores precisos apresentam elevada taxa de falsos positivos (Axelsson, 2000), e os alertas indevidos tendem a atingir quem foge ao padrão, como trabalhadores noturnos e pessoas com deficiência que usam

tecnologias assistivas. O erro não se distribui ao acaso. Quando modelos de linguagem resumem os incidentes, soma-se o risco de alucinação (Ji *et al.*, 2023). Na relação de emprego, esses escores operam em uma lógica de modulação em que a diferença individual pode converter-se em suspeita (Bruno, 2013; Zuboff, 2020). O efeito inibidor resultante é difícil de medir, mas foi observado nos acessos à Wikipédia após 2013 (Penney, 2016) e associado à dataficação (Büchi; Festic; Latzer, 2022). No ambiente de trabalho, pode desestimular o relato de incidentes (Ball, 2010).

No que diz respeito à finalidade e à cadeia de tratamento, usar a telemetria para medir produtividade é um uso secundário incompatível com a finalidade original (art. 6º, I; Solove, 2006). Quando o SOC ou o SIEM são terceirizados, o provedor atua como operador caso siga as instruções do controlador (arts. 5º, VII, e 39), que tem a responsabilidade de definir as finalidades e os meios essenciais do tratamento (art. 5º, VI). Se os dados forem processados no exterior, a transferência exige um mecanismo válido (ANPD, 2024d).

4.2. Índice Heurístico de Priorização

O índice de priorização é uma matriz heurística de triagem 3 × 3, inspirada na ISO/IEC 27005 (ISO, 2022), que combina propensão (P) e impacto (I), ambas classificadas de 1 a 3. A propensão mede a probabilidade de uma prática estar presente na configuração da ferramenta. A nota vale 3 quando a prática ocorre por omissão, 2 quando depende de decisão de política e 1 quando exige configuração específica. O impacto vale 1 quando o efeito sobre as pessoas é limitado e 2 quando afeta seus direitos sem agravante. Vale 3 quando há agravante do regulamento de dosimetria (ANPD,

2023a, art. 8º, §§ 2º e 3º), como dado sensível ou larga escala, ou efeito direto sobre o emprego ou a vida privada.

Da combinação dessas notas resultam quatro níveis. O nível crítico (9) ocorre quando ambas as notas são máximas, e o alto (6), quando uma é máxima e a outra intermediária. O nível é médio quando uma é máxima e a outra mínima (3) ou quando ambas são intermediárias (4), e baixo (1 ou 2) quando há uma nota mínima e nenhuma máxima. O produto P × I apenas identifica as células da matriz e não tem valor aritmético, pois a multiplicação de escalas ordinais pode igualar situações distintas (Cox Jr., 2008). No desenho proposto, Segurança, Privacidade e Jurídico pontuam de forma independente, com base no livro de códigos, e as divergências ficam registradas no RIPD.

Quatro das práticas descritas atingem o nível alto. A retenção ilimitada de *logs* de SIEM chega a esse nível por omissão (P 3 × I 2). A inspeção do conteúdo de mensagens pessoais por DLP, o reuso de *logs* para avaliar ou punir e o EDR irrestrito em dispositivos pessoais decorrem de decisões de política, mas têm impacto máximo (P 2 × I 3). O UEBA sem aviso fica no nível médio (P 2 × I 2), e os *logs* de autenticação pseudonimizados servem de linha de base (P 1 × I 1). O resultado é sensível às notas, pois alterar qualquer uma delas em um ponto muda o nível de todas as práticas, exceto a linha de base, como mostra a análise de sensibilidade do Quadro 16.

5. CRITÉRIOS DE EQUILÍBRIO E *FRAMEWORK* DE GOVERNANÇA

5.1. Diretrizes Jurídicas

Do teste de proporcionalidade (Alexy, 2008) partem as diretrizes jurídicas do *framework*, e as etapas do teste se convertem em

perguntas sobre a configuração do SOC. A adequação questiona se o dado contribui para detectar a ameaça definida na finalidade. Assim, excluem-se os campos que nenhuma regra de detecção utiliza. A necessidade exige, entre meios igualmente eficazes, o menos gravoso, como usar metadados em vez do conteúdo das mensagens. A proporcionalidade, em sentido estrito, avalia o ganho de detecção contra a intrusão que permanece. Como essas etapas se assemelham ao teste de balanceamento que a ANPD orienta para o legítimo interesse (ANPD, 2024a) e aos fatores do caso Bărbulescu (Conselho da Europa, 2017), as análises podem ser consolidadas em um único documento, o qual atende, simultaneamente, aos três referenciais.

A responsabilização (art. 6º, X) soma o ônus de comprovar que medidas eficazes foram adotadas (Bioni, 2022), e uma decisão de proporcionalidade sem documento que a registre dificilmente se sustenta em uma fiscalização. Por isso, o *framework* enfatiza os artefatos. O encarregado é consultado sobre as configurações, mas a decisão sobre os meios de tratamento cabe ao controlador (ANPD, 2024c). Na relação de emprego, a demonstração inclui também as salvaguardas que limitam o poder diretivo, como a proibição de usar alertas para disciplina direta e a revisão humana das medidas que afetam o trabalhador (Oliveira Neto, 2023).

5.2. Diretrizes Técnicas

Especificadas em detalhe no Apêndice B, as salvaguardas técnicas se transformam em controles de engenharia que seguem o *Privacy by Design* (Cavoukian, 2009) e as estratégias de Hoepman (2014). Privilegia-se a privacidade que vem da própria arquitetura do sistema (*privacy-by-architecture*), que é menos sujeita a falhas na

observância de políticas internas (Spiekermann; Cranor, 2009). O primeiro corte ocorre no ciclo de vida dos *logs*: cada classe de telemetria recebe um prazo fechado de retenção; ao fim desse prazo, os eventos sem indicadores de comprometimento (IoC) são rapidamente descartados. As partições do repositório são, ainda, cifradas com chaves próprias, e a destruição das chaves ao final do prazo provoca o apagamento criptográfico, ou *crypto-shredding* (Chandramouli; Hibbard, 2025).

Logo na ingestão entra o segundo freio técnico: a pseudonimização dos identificadores. Essa técnica faz com que o dado não possa ser associado ao titular, a menos que seja usada informação adicional mantida separadamente, conforme a LGPD (art. 13, § 4º). O conceito foi criado para estudos em saúde pública, mas aqui serve como salvaguarda (arts. 6º, III e VII, e 46). O identificador recebe um código de autenticação de mensagem com chave (HMAC), calculado em módulo de segurança de *hardware* (HSM) (NIST, 2008), e o endereço IP é cifrado com preservação de prefixo pelo esquema Crypto-PAn (Xu *et al.*, 2002). O HMAC gera, com chave secreta, um pseudônimo determinístico que não pode ser revertido ao identificador original. No entanto, há um ponto frágil. Como quem detém a chave pode recalcular os pseudônimos de todos os identificadores corporativos, a proteção depende da guarda da chave e do controle das informações auxiliares. A reidentificação autorizada requer, por isso, um cofre separado, sob controle duplo. A Crypto-PAn, ao contrário, pode ser revertida com a chave e, ao manter as relações de sub-rede, permite inferir a topologia da rede (Coull *et al.*, 2007). Para o Comitê Europeu para a Proteção de Dados (EDPB, na sigla em inglês), dados tratados dessa forma continuam pessoais para quem detém a chave (EDPB, 2025). Em contrapartida, o Tribunal de Justiça da União Europeia (TJUE) admite que esses dados podem não ser

considerados pessoais pelo destinatário sem meios razoáveis de reidentificação (União Europeia, 2025). Na LGPD, o provedor de SOC que recebe esses dados pseudonimizados é, em regra, operador.

No Passo 3, decide-se o tratamento de cada campo com base nas regras de detecção do Passo 1. O campo que nenhuma regra utiliza, ou que é sensível sem hipótese do art. 11, é suprimido, e aquele que as regras empregam apenas em granularidade menor é agregado. A pseudonimização é reservada aos campos que precisam vincular eventos à mesma conta. O restante do *framework* aplica *Transport Layer Security* (TLS) 1.3 em trânsito (McKay; Cooper, 2019), AES-256-GCM em repouso (Barker, 2020), controle de acesso baseado em papéis (RBAC), autenticação multifator e trilha de auditoria das consultas, protegida contra alteração. Essa trilha de auditoria constitui o principal controle previsto contra o abuso de privilégio interno.

Para as organizações menores, a adoção de HSM, ambientes de execução confiáveis e cofres de *tokens* pesa proporcionalmente mais, devido aos custos financeiros e ao acréscimo de latência que implica. No perfil reduzido (R5), um serviço gerenciado de chaves em nuvem, sob controle do cliente, substitui o HSM. O mínimo indispensável passa a ser separar a chave dos dados e registrar as reidentificações.

A modelagem STRIDE + LINDDUN revela onde essas decisões aliviam ou agravam as ameaças à privacidade. Dos oito pares representativos do Quadro 2, três são de convergência, quatro de tensão e um de conflito. A convergência aparece, por exemplo, quando o TLS mútuo protege a ingestão e reduz a exposição de dados a terceiros. Já a correlação por conta, necessária contra

Spoofing, facilita o *Linking* e gera tensão, atenuada pelo pseudônimo determinístico. O único conflito está no registro de ações privadas, pois o não repúdio, exigido pela segurança, pressupõe que cada ação possa ser atribuída a seu autor sem que ele possa negá-la, e a privacidade protege justamente a possibilidade de o titular negar plausivelmente uma ação privada. O impasse é estrutural. Entre os controles examinados neste estudo, nenhum assegura as duas coisas para a mesma ação (Deng *et al.*, 2011). Uma decisão de escopo contorna o problema ao restringir o registro nominal às ações privilegiadas, e o Quadro 18 detalha a configuração correspondente nos coletores de EDR e SIEM.

Quadro 2. Relações entre ameaças STRIDE e LINDDUN por elemento do *pipeline* do SOC (versão sintética)

Elemento	Par STRIDE / LINDDUN	Relação	Conciliação ou controle complementar
Fonte (estações)	*Spoofing* / *Linking* e *Identifying*	Tensão	Pseudônimo determinístico e cofre de correspondência
Fonte (rede)	*Denial of Service* / *Detecting* e *Linking*	Tensão	Agregação por sub-rede e fluxo por dispositivo restrito a alertas
Ingestão	*Information Disclosure* / *Data Disclosure*	Convergência	TLS mútuo e higienização de campos livres
Armazenamento	*Tampering* / *Non-compliance*	Tensão	Expiração por partição e apagamento criptográfico

Armazenamento	*Repudiation* / *Non-repudiation*	Conflito	Decisão de escopo que restringe o não repúdio a ações privilegiadas
Armazenamento e consulta	*Information Disclosure* / *Data Disclosure*	Convergência	AES-256-GCM, RBAC e trilha de auditoria das consultas
Consulta (UEBA)	*Elevation of Privilege* / *Detecting* e *Unawareness and Unintervenability*	Tensão	Aviso interno e revisão humana
Reidentificação	*Elevation of Privilege* / *Identifying*	Convergência	Separação de funções, controle duplo e relatório ao encarregado

Fonte: Elaborado pelos autores (2026), com base em Shostack (2014), Deng *et al.* (2011), Robles-González, Parra-Arnau e Forné (2020) e Sion *et al.* (2025). Pares representativos de uma matriz muitos-para-muitos, detalhada no Quadro 18.

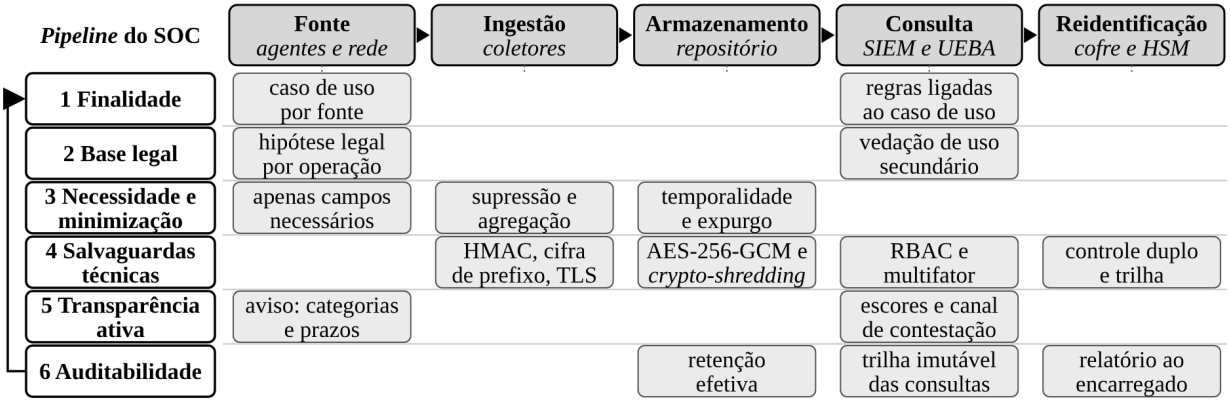
5.3. *Framework* em Seis Passos e Posicionamento

O *framework* de seis passos é estruturado para organizar as diretrizes de coleta de dados, com orientação das áreas de Segurança, Tecnologia da Informação, Jurídico e Privacidade. Os Passos 1 e 2 definem se a coleta de dados é permitida, baseando-se na relação entre a fonte de telemetria e uma ameaça real, e entre a operação e uma hipótese legal válida. A forma como os dados serão coletados, campo por campo, é definida nos Passos 3 e 4, com prazos e medidas de proteção que atuam em pontos distintos do *pipeline* (Figura 1). Por sua vez, os Passos 5 e 6 cuidam da

transparência, garantindo que o titular dos dados e o auditor tenham visibilidade sobre as decisões tomadas. Mudar regra, fonte ou fornecedor reinicia o ciclo. A cada passo correspondem uma pergunta-chave e um artefato (Quadro 3), entendido como o documento aprovado que registra uma decisão, como o dicionário de dados. Já a consulta de um analista a um pseudônimo fica registrada na trilha de auditoria, e a proporção de campos pseudonimizados constitui um indicador de auditoria. Os artefatos, detalhados nos Quadros 7 e 8 e na Figura 2, também servem como evidência para cumprir controles da ISO/IEC 27002, da ISO/IEC 27701 e do NIST CSF 2.0, conforme indicado no Quadro 14.

Nem todos os passos têm o mesmo peso. Documentar a finalidade, criptografar os dados, limitar o acesso e informar o titular (Passos 1, 4 e 5) são requisitos relativamente claros e não costumam gerar disputas. As controvérsias surgem principalmente em torno da hipótese legal para análise comportamental e para sinais biométricos (Passo 2), do prazo e da precisão com que os dados são armazenados (Passo 3), e da reidentificação controlada (Passos 4 e 6). É sobre esses pontos que a análise seguinte será focada.

Figura 1. *Framework* em seis passos e seus pontos de atuação no *pipeline* do SOC



Fonte: Elaborada pelos autores (2026).

Quadro 3. Síntese do *framework*: pergunta-chave, dispositivos, artefato e indicador de auditoria por passo

Passo	Pergunta-chave	Dispositivos da LGPD	Artefato	Indicador de auditoria
1 Finalidade	Que ameaça justifica cada coleta?	Art. 6º, I, e art. 37.	Registro de casos de uso do SIEM, integrado ao registro das operações.	Fontes sem caso de uso.
2 Base legal	Que hipótese ampara cada operação?	Arts. 7º, 10, 11 e 38.	Registro de hipótese legal e teste de balanceamento, com RIPD em alto risco.	Operações sem hipótese documentada.
3 Necessidade e minimização	Que campos e prazos são necessários?	Art. 6º, III, e arts. 15 e 16.	Dicionário de dados de ingestão e tabela de temporalidade.	Dados pessoais por evento e retenção efetiva.
4 Salvaguardas técnicas	Como proteger o que é coletado?	Arts. 46 a 49.	Especificação de salvaguardas (pseudonimização, criptografia e acesso).	Campos pseudonimizados e acessos privilegiados revisados.
5 Transparência ativa	O que o titular sabe e como contesta?	Art. 6º, VI, e arts. 9º, 18 e 20.	Aviso interno e canal de contestação, com categorias, finalidades e prazos.	Contestações recebidas e respondidas.

6 Auditabilidade	Como demonstrar o que foi feito?	Art. 6º, X, e art. 50.	Trilha de auditoria das consultas, relatório de reidentificações e RIPD versionado.	Reidentificações e justificativas por período.

Fonte: Elaborado pelos autores (2026).

5.4. Demonstração e Avaliação *Ex Ante*

Como primeiro cenário, examina-se uma instituição financeira hipotética, que conta com três mil colaboradores em regime híbrido, cuja ferramenta de UEBA reúne cinco atributos pessoais: o identificador, o IP, o conteúdo das mensagens, a dinâmica de digitação e a geolocalização. Essa configuração de referência representa o pior caso plausível. No Passo 1, a finalidade restringe a coleta apenas à detecção de credenciais comprometidas e de movimentações anômalas de dados classificados. Em relação à base legal, os controles impostos pela Resolução CMN nº 4.893/2021 baseiam-se na obrigação regulatória, enquanto a análise comportamental, que vai além desse conjunto, depende do legítimo interesse, exigindo teste de balanceamento e RIPD. A velocidade de digitação é excluída já no Passo 2, porque a ferramenta compara o ritmo de digitação ao perfil da conta para verificar se quem digita é o titular. Com esse uso, o sinal satisfaz o teste funcional adotado e torna-se biométrico, sem respaldo em nenhuma hipótese do art. 11, visto que o consentimento dificilmente é livre no emprego e nenhuma norma impõe esse tratamento. A alínea g, lida de forma restritiva, limita-se ao cadastro, e o legítimo interesse não abrange dados sensíveis.

Ao fim dos Passos 2 a 4, dois atributos são suprimidos, um é agregado e dois são pseudonimizados, e podem ser identificados apenas mediante informação mantida em separado (Quadro 4). Cada decisão trata de uma ameaça ao LINDDUN. Sob a mesma chave, o pseudônimo mantém a correlação necessária para a detecção de *Spoofing* e reduz o risco de *Identifying*. O IP cifrado e a agregação geográfica contêm *Linking* e *Detecting*, enquanto o expurgo afasta *Non-compliance* e o aviso com revisão humana reduz *Unawareness and Unintervenability*.

Quadro 4. Evento de UEBA antes e depois dos Passos 2 a 4 no cenário bancário

Atributo ou parâmetro	**Configuração de referência**	**Após o *framework***	**Origem da decisão**
Identificador (user_id)	acesse o artigo original para visualizar o e-mail	Pseudônimo HMAC-SHA-256, com chave em HSM (usr_9f8a7b6c, em forma abreviada). Reidentificação autorizada apenas pelo cofre (Passo 6).	Passo 4
IP de origem (src_ip)	203.0.113.45	IP cifrado com preservação de prefixo, recuperável apenas com a chave.	Passo 4
Conteúdo de mensagens	Corpo, anexos e área de transferência.	Suprimido. Ficam registrados o volume (bytes_out) e o *hash* de arquivo classificado.	Passo 3
Dinâmica de digitação	Captura contínua.	Desativada.	Passo 2, confirmada no Passo 3

Geolocalização	Coordenadas ou rede doméstica.	Agregada por unidade federativa.	Passo 3, com granularidade definida pelo cenário
Retenção (parâmetro)	Indefinida.	12 meses para autenticação (3 em acesso imediato) e 6 meses para telemetria sem IoC, com preservação seletiva de incidentes.	Passo 3 (Seção 6.1)

Fonte: Elaborado pelos autores (2026). Identificadores fictícios, de faixas reservadas para documentação (Eastlake 3rd; Panitz, 1999; Arkko; Cotton; Vegoda, 2010). A LGPD não fixa prazos gerais de retenção, e a regulação do CMN deixa à instituição defini-los por tipo de processamento (Conselho Monetário Nacional, 2025).

Permanecem os campos exigidos por regras típicas do Passo 1 (falhas sucessivas de autenticação, origem improvável e volume anômalo de saída). Esses campos são horário, pseudônimo, IP cifrado, unidade federativa, volume e resultado da autenticação. Soma-se a isso, para unidades com poucos usuários, a proposta de agregar a localização por região sempre que houver menos de $k = 10$ contas ativas, na lógica do *k*-anonimato (Sweeney, 2002). Contra ataques de interseção no teletrabalho (Ganta; Kasiviswanathan; Smith, 2008), as visões de tendência agrupam os horários em intervalos de 15 ou 30 minutos.

Parte da hipótese de preservação da detecção pode ser analisada por argumento, ao se separarem as propriedades dos esquemas das condições de implementação. Com uma chave fixa, a Crypto-PAn é uma permutação dos endereços IPv4 que preserva prefixos (Xu *et*

al., 2002). Embora o HMAC, que transforma entradas de tamanho arbitrário em saídas de tamanho fixo (NIST, 2008), não garanta injetividade, as colisões tornam-se insignificantes no espaço reduzido de identificadores de uma organização e sem truncamento excessivo da saída. Sob essas premissas (e desde que a chave, a normalização dos identificadores e a transformação das listas e sub-redes usadas nas regras sejam as mesmas), regras de igualdade, de contagem por conta ou de pertinência a sub-rede geram, em tese, os mesmos alertas. Já as regras sobre padrões textuais do identificador ou sobre faixas de endereços desalinhadas dos prefixos não se preservam. Nada disso foi medido empiricamente. O risco de perda de sinal concentra-se nos enriquecimentos que pressupõem o valor original, como a consulta a listas de reputação; nas agregações do Passo 3, capazes de apagar sinais finos; e na rotação de chaves, que rompe a vinculação entre períodos. Para reduzir essas perdas, os enriquecimentos ocorrem na ingestão, antes da pseudonimização, e a janela de dupla chave proposta na Seção 6.1 diminui a ruptura entre períodos. Menges *et al.* (2021) examinaram o efeito da pseudonimização sobre a detecção em SIEM, e a medição desse efeito no cenário do presente trabalho integra a prova de conceito prevista na agenda de validação.

No Passo 5, o aviso interno é escrito sem revelar regras de detecção. No Passo 6, a trilha de auditoria cobre consultas e reidentificações, com dupla aprovação e relatório trimestral ao encarregado (Quadros 10 e 11). Juntamente com o cenário de pequena empresa, descrito no Apêndice D, as evidências desses passos mostram que os requisitos de ancoragem normativa (R1) e de compatibilidade com referenciais (R6) são atendidos. Os requisitos R2 a R4 são atendidos no desenho. No entanto, a proporcionalidade ao porte (R5) só é atendida

parcialmente, porque o perfil reduzido ainda não tem estimativa de custos.

6. DISCUSSÃO

6.1. Interdependência e *Trade-Offs*

Diante dos cenários analisados, a ideia de que segurança e privacidade são opostas (Solove, 2011) sustenta-se apenas até certo ponto. É verdade que a própria LGPD inclui a segurança como um princípio (art. 6º, VII) e que bases enxutas reduzem a superfície de dano caso o SIEM seja invadido e exfiltrado (Menges *et al.*, 2021). No entanto, no dia a dia de um SOC, essa harmonia não ocorre de forma automática; ela resulta de escolhas finas de configuração e esbarra em quatro obstáculos, mesmo após a aplicação do *framework*.

O atrito mais visível opõe o dever de minimização à janela de investigação forense. Segundo a Mandiant (2026), o tempo médio global de permanência de invasores antes da detecção foi de 14 dias em 2025, mas chegou a 122 dias em casos de espionagem e de falsos trabalhadores de TI norte-coreanos. Invasões com o *backdoor* BRICKSTORM duraram cerca de 400 dias. Esses dados são estimativas de mercado e refletem apenas a amostra de incidentes investigados por uma única empresa, sem pretensão de validade estatística universal. No cenário bancário, os seis meses de telemetria sem IoC superam os 122 dias, mas intrusões mais longas contariam apenas com os 12 meses de registros de autenticação. Os prazos do cenário coincidem com os do Payment Card Industry Data Security Standard (PCI DSS), restrito a dados de cartão (PCI Security Standards Council, 2024), e com a faixa que a Commission Nationale de l'Informatique et des Libertés (CNIL) recomenda para registros de

acesso (CNIL, 2021). Para calibrar esse prazo, propõe-se a seguinte hipótese operacional: reter metadados pseudonimizados até o percentil 75 ou 90 do tempo de permanência de invasores observado no setor. Se não houver essa distribuição setorial, o prazo adotaria o maior valor entre o dobro da mediana para ameaças persistentes (244 dias) e o percentil 90 do tempo de detecção nos incidentes e exercícios de *red team* da própria instituição. Trata-se de um critério verificável nos registros internos.

Na pseudonimização, a tensão é diferente, porque pseudônimos determinísticos preservam a correlação, mas aumentam a vinculabilidade. A rotação de chaves reduz esse risco, mas rompe as séries históricas e dificulta a detecção de exfiltrações lentas e de baixo volume (*low-and-slow*), cuja duração pode exceder o ciclo de rotação. O ganho de privacidade custa visibilidade. Para esses casos, propõe-se uma janela de transição com dupla chave. Durante um prazo limitado, o HSM mantém a chave anterior e a nova, e o cofre converte o pseudônimo antigo no novo sem expor o identificador aos analistas. A conversão serve apenas para recalcular os contadores agregados de risco das contas com indicadores parciais acima de um limiar fixado no RIPD. Nas demais contas, a chave antiga é destruída e o vínculo entre períodos se perde. Cada conversão fica registrada na trilha de auditoria do Passo 6.

A transparência também encontra limites, pois divulgar integralmente as regras de detecção facilitaria sua evasão. A própria LGPD protege os segredos comerciais e industriais (art. 6º, VI). Essa ressalva legal, no entanto, agrava a assimetria informacional inerente à relação de emprego: ao contestar um alerta, o trabalhador desconhece o critério que o gerou, o que inviabiliza, na prática, a demonstração de um eventual erro material. Restam-lhe a revisão

humana e, quando a decisão decorrer de tratamento automatizado, a auditoria que a ANPD pode realizar para verificar aspectos discriminatórios (art. 20, § 2º). O aviso do Passo 5 busca equilibrar esses interesses ao descrever categorias de dados e finalidades do monitoramento, sem expor as minúcias das regras de detecção.

Há ainda limites que a tecnologia não supera, pois a privacidade não se traduz integralmente em código (Koops; Leenes, 2014). Parte das garantias depende de negociação coletiva, como na Itália, onde o controle remoto de trabalhadores demanda acordo sindical (Garante per la Protezione dei Dati Personali, 2024). No Brasil, a norma coletiva possui reconhecimento constitucional e legal (art. 7º, XXVI, da CF; art. 611-A da CLT). Na leitura aqui proposta, as salvaguardas pactuadas nessas convenções reforçam as legítimas expectativas do titular, mas não substituem o teste de balanceamento. Vale ressaltar que o próprio *framework* corre o risco de converter-se em burocracia documental caso seus artefatos não sejam efetivamente auditados (Passo 6).

6.2. Prática Regulatória e Experiência Comparada

Até a data de corte, a pesquisa não localizou decisão da ANPD estritamente sobre monitoramento de segurança cibernética de colaboradores. Segundo Barzotto e Siciliani (2025), a questão permanece incerta e exige atuação regulamentar preventiva da autoridade. Precedentes de outros contextos oferecem, porém, parâmetros úteis. Na primeira sanção aplicada, o caso Telekall Infoservice, a autarquia puniu o tratamento de dados desprovido de hipótese legal (ANPD, 2023c), risco cuja prevenção é justamente o objeto do Passo 2. No caso Tools for Humanity, a ANPD manteve suspensa a compensação financeira pela coleta de íris (ANPD,

2025a), por entender que a contrapartida compromete a liberdade do consentimento. Esse raciocínio aproxima-se da reserva feita na Seção 2.3 quanto à validade do consentimento nas relações de emprego.

Na Europa, há mais decisões aplicáveis. A CNIL multou a Amazon France Logistique por indicadores de inatividade dos trabalhadores e pela retenção desses dados por 31 dias (CNIL, 2023), e o Conselho de Estado reduziu a multa, mas manteve a violação da minimização (França, 2025). Na Itália, o Garante fixou em 21 dias a referência para metadados de *e-mail* de trabalhadores (Garante per la Protezione dei Dati Personali, 2024). Ainda que o caso Amazon tratasse de monitoramento de desempenho, nos dois precedentes a atenção centrou-se no prazo de guarda e no nível de detalhe dos dados. Esse ponto comum reforça a importância do Passo 3, pois a tabela de temporalidade e a justificativa campo a campo tendem a ser as primeiras evidências examinadas em uma fiscalização.

6.3. Limites e Agenda de Validação

Os limites começam pelo método. A revisão é narrativa, sem critério formal de saturação nem contagem dos resultados brutos das buscas, e a codificação coube a um único pesquisador. As notas do índice de priorização resultam de julgamento fundamentado, o critério de retenção por percentil ainda aguarda calibração com dados setoriais e as propriedades criptográficas invocadas na demonstração decorrem da especificação dos esquemas e carecem de testes de implementação. Por ser *ex ante*, a avaliação também não comprova a eficácia do artefato em uso. A principal hipótese ainda não testada é a de que os Passos 3 e 4 preservam a sensibilidade e a taxa de falsos positivos das regras do Passo 1.

Prevê-se testar essa hipótese em duas etapas. A primeira delas consistirá em uma prova de conceito que executará as regras do Passo 1, antes e depois das transformações, sobre bases públicas como o Insider Threat Test Dataset (Lindauer, 2020) e os eventos do Los Alamos National Laboratory (Kent, 2015). Em seguida, o experimento comparará a sensibilidade e a taxa de falsos positivos nas duas condições por meio do teste pareado de McNemar. A segunda etapa, por sua vez, envolverá a participação de sujeitos humanos: após apreciação ética, um painel Delphi com encarregados de dados, analistas de SOC e advogados julgará a utilidade e a viabilidade do *framework*, além da completude de seus artefatos. Posteriormente, um estudo de caso em uma organização real medirá a sensibilidade e a taxa de falsos positivos em ambiente de produção, replicando o método da prova de conceito. A agenda estendida prevê, ainda, a revisão das premissas criptográficas por um especialista independente; a atualização da revisão de literatura guiada pelo protocolo prospectivo do Quadro 5 (com recodificação às cegas de uma amostra da matriz); e o depósito integral da matriz e do *corpus* em repositório aberto.

7. CONCLUSÃO

Em resposta à pergunta de pesquisa, os critérios identificados exigem que cada dado coletado pelo SOC esteja ligado a uma ameaça definida e a uma hipótese legal própria e se limite ao que as regras de detecção efetivamente usam. Também é necessário que esse dado receba salvaguardas técnicas e esteja visível ao titular e verificável pelo auditor. O estudo atinge os quatro objetivos específicos fixados na introdução. O levantamento normativo mostra que a LGPD não oferece hipótese genérica para o monitoramento defensivo. Com a interpretação adotada, o dever de segurança do

art. 46 protege, no máximo, o registro essencial para a proteção, e a análise comportamental precisa ter um fundamento próprio. Entre as práticas que mais expõem os titulares, destacam-se a retenção sem expurgo, a inspeção de conteúdo, o reuso disciplinar dos registros e o EDR em dispositivos pessoais.

No setor bancário, dos cinco atributos pessoais da configuração de referência, o conteúdo das mensagens é removido e a dinâmica de digitação é excluída por funcionar como dado biométrico sem hipótese do art. 11. A geolocalização é agregada por unidade federativa, e o identificador e o IP são pseudonimizados. Nem todos os riscos são eliminados. Continuam existindo riscos que o *framework* apenas reduz, como a vinculabilidade criada por pseudônimos determinísticos, a inferência de topologia permitida pela cifra com preservação de prefixo e o isolamento de contas pela interseção de horários no teletrabalho. Na matriz STRIDE + LINDDUN, apenas o não repúdio de ações privadas não encontra conciliação entre os controles examinados e exige uma decisão de escopo, enquanto nos demais pares a compatibilidade resulta de escolhas de configuração. A tese do falso dilema confirma-se, assim, apenas em parte. Em um mesmo SIEM, a fronteira entre defesa e vigilância passa pelos campos coletados, pelo tempo de guarda e pela possibilidade de reidentificação dos titulares.

Como a avaliação é apenas *ex ante*, os resultados têm alcance limitado. A preservação da capacidade de detecção depende de uma prova de conceito, pois as agregações, os enriquecimentos que exigem o valor original e a rotação de chaves podem apagar sinais cuja perda só a medição revela. A calibração dos prazos de retenção exige distribuições do tempo de permanência de invasores em organizações brasileiras, hoje raramente divulgadas. Ainda falta ouvir

os trabalhadores. A escuta permitiria saber se a transparência e a revisão humana diminuem o efeito inibidor e se os escores de UEBA geram taxa mais elevada de falsos positivos em perfis atípicos, como trabalhadores noturnos e pessoas com deficiência. Também é necessário expandir a análise ao setor de saúde, em que a telemetria tende a coletar dados sensíveis, e ao setor público, que está sujeito ao art. 23 da LGPD. Enquanto essa agenda não for concluída, o *framework* oferece um procedimento documentável, com eficácia ainda não comprovada no uso prático, que já permite a controladores e encarregados exigirem, para cada campo coletado pelo SOC, uma justificativa por escrito que o vincule a uma ameaça concreta e a uma hipótese legal, com prazo de descarte definido na tabela de temporalidade.

REFERÊNCIAS BIBLIOGRÁFICAS

ACIOLY, Luis Henrique de Menezes; SILVA, Matheus Fernandes da; MONTEIRO NETO, João Araújo. A Emenda Constitucional nº 115 de 10 de fevereiro de 2022 e o enforcement da proteção de dados pessoais no Brasil. **Revista de Investigações Constitucionais,** Curitiba, v. 11, n. 3, e275, set./dez. 2024. DOI: https://doi.org/10.5380/rinc.v11i3.92117.

AJUNWA, Ifeoma; CRAWFORD, Kate; SCHULTZ, Jason M. Limitless worker surveillance. **California Law Review,** Berkeley, v. 105, n. 3, p. 735-776, 2017. DOI: https://doi.org/10.15779/Z38BR8MF94.

AL-SHEHARI, Taher Ali *et al.* Enhancing insider threat detection in imbalanced cybersecurity settings using the density-based local outlier factor algorithm. **IEEE Access,** Piscataway, v. 12, p. 34820-34834, 2024. DOI: https://doi.org/10.1109/ACCESS.2024.3373694.

ALEMANHA. Bundesverfassungsgericht (Erster Senat). **Urteil vom 15. Dezember 1983, 1 BvR 209/83 u. a. (Volkszählungsurteil).** Julgado em 15 dez. 1983. Entscheidungen des Bundesverfassungsgerichts, Tübingen, v. 65, p. 1, 1983.

ALEXY, Robert. **Teoria dos direitos fundamentais.** Tradução de Virgílio Afonso da Silva. São Paulo: Malheiros, 2008.

ARKKO, Jari; COTTON, Michelle; VEGODA, Leo. **IPv4 address blocks reserved for documentation.** [*S. l.*]: Internet Engineering Task Force, 2010. (RFC 5737). DOI: https://doi.org/10.17487/RFC5737.

ARTICLE 29 DATA PROTECTION WORKING PARTY. **Opinion 2/2017 on data processing at work:** WP 249. Brussels: European Commission, 2017. Disponível em: https://ec.europa.eu/newsroom/article29/items/610169. Acesso em: 28 out. 2026.

ARTICLE 29 DATA PROTECTION WORKING PARTY. **Opinion 3/2012 on developments in biometric technologies:** WP 193. Brussels: European Commission, 2012. Disponível em: https://www.aepd.es/sites/default/files/2019-12/wp193_en.pdf. Acesso em: 3 nov. 2026.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **ABNT NBR ISO/IEC 27001:** segurança da informação, segurança cibernética e proteção à privacidade - sistemas de gestão da segurança da informação - requisitos. Rio de Janeiro: ABNT, 2022a.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **ABNT NBR ISO/IEC 27002:** segurança da informação, segurança

cibernética e proteção à privacidade - controles de segurança da informação. Rio de Janeiro: ABNT, 2022b.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **ABNT NBR ISO/IEC 27037:** tecnologia da informação - técnicas de segurança - diretrizes para identificação, coleta, aquisição e preservação de evidência digital. Rio de Janeiro: ABNT, 2013.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **ABNT NBR ISO/IEC 27701:** técnicas de segurança - extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação - requisitos e diretrizes. Rio de Janeiro: ABNT, 2019.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). Conselho Diretor. **Despacho Decisório PR/ANPD nº 6/2025:** recurso administrativo interposto por Tools for Humanity (World ID); Voto nº 1/2025/DIR-MW/CD. Diário Oficial da União: Brasília, DF, 11 fev. 2025a. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/deliberacoes-do-conselho-diretor-1/circuitos-deliberativos-ano-2025/cd-10-2025-votos.pdf/@@download/file. Acesso em: 2 nov. 2026.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). Coordenação-Geral de Fiscalização. **3º Relatório de Ciclo de Monitoramento:** 2º semestre de 2023 - 1º semestre de 2025. Brasília, DF: ANPD, 2025b. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/RelatorioCiclodeMonitoramento20232025.pdf. Acesso em: 3 nov. 2026.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). Coordenação-Geral de Fiscalização. **Decisão no Processo Administrativo Sancionador nº 00261.000489/2022-62:** Telekall

Infoservice. Diário Oficial da União: seção 1, Brasília, DF, 6 jul. 2023c. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/sei_00261-000489_2022_62_decisao_telekall_inforservice.pdf. Acesso em: 28 out. 2026.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). Coordenação-Geral de Normatização. **Nota Técnica nº 23/2025/CON1/CGN/ANPD:** consolidação das contribuições recebidas na tomada de subsídios sobre dados pessoais sensíveis - dados biométricos. Brasília, DF: ANPD, 26 nov. 2025c. Disponível em: https://www.gov.br/anpd/pt-br/acesso-a-informacao/participacao-social/outras-acoes/ts-01-2025/nota-tecnica-no-23-2025-con1-cgn-anpd.pdf. Acesso em: 9 nov. 2026.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Guia orientativo:** hipóteses legais de tratamento de dados pessoais - legítimo interesse. Brasília, DF: ANPD, fev. 2024a. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia_orientativo_hipoteses_legais_tratamento_de_dados_pessoais_legitimo_interesse. Acesso em: 28 out. 2026.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Relatório de Impacto à Proteção de Dados Pessoais (RIPD):** perguntas e respostas. Brasília, DF: ANPD, 6 abr. 2023b. Disponível em: https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/relatorio-de-impacto-a-protecao-de-dados-pessoais-ripd. Acesso em: 3 nov. 2026.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Resolução CD/ANPD nº 15, de 24 de abril de 2024.** Aprova o Regulamento de Comunicação de Incidente de Segurança. Diário Oficial da União: seção 1, Brasília, DF, 26 abr. 2024b. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-15-de-24-de-abril-de-2024-556243024. Acesso em: 2 nov. 2026.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Resolução CD/ANPD nº 18, de 16 de julho de 2024.** Aprova o Regulamento sobre a atuação do encarregado pelo tratamento de dados pessoais. Diário Oficial da União: seção 1, Brasília, DF, n. 136, p. 42, 17 jul. 2024c. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-18-de-16-de-julho-de-2024-572632074. Acesso em: 2 nov. 2026.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Resolução CD/ANPD nº 19, de 23 de agosto de 2024.** Aprova o Regulamento de Transferência Internacional de Dados e o conteúdo das cláusulas-padrão contratuais. Diário Oficial da União: seção 1, Brasília, DF, 23 ago. 2024d. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-19-de-23-de-agosto-de-2024-580095396. Acesso em: 2 nov. 2026.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Resolução CD/ANPD nº 2, de 27 de janeiro de 2022.** Aprova o Regulamento de aplicação da Lei nº 13.709, de 14 de agosto de 2018, para agentes de tratamento de pequeno porte. Diário Oficial da União: seção 1, Brasília, DF, 28 jan. 2022. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-2-de-27-de-janeiro-de-2022-376562019. Acesso em: 2 nov. 2026.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Resolução CD/ANPD nº 4, de 24 de fevereiro de 2023.** Aprova o Regulamento de Dosimetria e Aplicação de Sanções Administrativas. Diário Oficial da União: seção 1, Brasília, DF, 27 fev. 2023a. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-4-de-24-de-fevereiro-de-2023-466146077. Acesso em: 2 nov. 2026.

AXELSSON, Stefan. The base-rate fallacy and the difficulty of intrusion detection. **ACM Transactions on Information and System Security,** New York, v. 3, n. 3, p. 186-205, 2000. DOI: https://doi.org/10.1145/357830.357849.

BALL, Kirstie. Workplace surveillance: an overview. **Labor History,** Abingdon, v. 51, n. 1, p. 87-106, 2010. DOI: https://doi.org/10.1080/00236561003654776.

BANCO CENTRAL DO BRASIL (BCB). **Resolução BCB nº 538, de 18 de dezembro de 2025.** Altera a Resolução BCB nº 85, de 8 de abril de 2021. Brasília, DF: BCB, 2025. Disponível em: https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=538. Acesso em: 2 nov. 2026.

BANCO CENTRAL DO BRASIL (BCB). **Resolução BCB nº 85, de 8 de abril de 2021.** Dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições de pagamento autorizadas a funcionar pelo Banco Central do Brasil. Brasília, DF: BCB, 2021. Disponível em: https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?

tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=85. Acesso em: 2 nov. 2026.

BARKER, Elaine. **Recommendation for key management:** part 1 - general. Gaithersburg: National Institute of Standards and Technology, 2020. (NIST Special Publication 800-57 Part 1, Rev. 5). DOI: https://doi.org/10.6028/NIST.SP.800-57pt1r5.

BARZOTTO, Luciane Cardoso; SICILIANI, Bruna Casimiro. Responsabilidade preventiva e proteção de dados na relação de emprego: o papel regulamentar da ANPD. **Revista de Direito do Trabalho e Seguridade Social,** São Paulo, v. 51, n. 243, p. 187-197, set./out. 2025. Disponível em: https://hdl.handle.net/20.500.12178/265126. Acesso em: 3 nov. 2026.

BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. Rio de Janeiro: Forense, 2019.

BIONI, Bruno Ricardo. **Regulação e proteção de dados pessoais:** o princípio da accountability. Rio de Janeiro: Forense, 2022.

BISKUP, Joachim; FLEGEL, Ulrich. Transaction-based pseudonyms in audit data for privacy respecting intrusion detection. *In*: INTERNATIONAL WORKSHOP ON RECENT ADVANCES IN INTRUSION DETECTION (RAID), 3., 2000, Toulouse. **Proceedings** [...]. Berlin: Springer, 2000. p. 28-48. (Lecture Notes in Computer Science, v. 1907). DOI: https://doi.org/10.1007/3-540-39945-3_3.

BOWEN, Glenn A. Document analysis as a qualitative research method. **Qualitative Research Journal,** Bingley, v. 9, n. 2, p. 27-40, 2009. DOI: https://doi.org/10.3316/QRJ0902027.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988.** Brasília, DF: Presidência da República, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 27 out. 2026.

BRASIL. Câmara dos Deputados. **Projeto de Lei nº 2.338, de 2023.** Dispõe sobre o desenvolvimento, o fomento e o uso ético e responsável da inteligência artificial com base na centralidade da pessoa humana. Brasília, DF: Câmara dos Deputados, 2023c. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao/?idProposicao=2487262. Acesso em: 2 nov. 2026.

BRASIL. **Decreto nº 11.856, de 26 de dezembro de 2023.** Institui a Política Nacional de Cibersegurança e o Comitê Nacional de Cibersegurança. Brasília, DF: Presidência da República, 2023a. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/D11856.htm. Acesso em: 2 nov. 2026.

BRASIL. **Decreto-Lei nº 5.452, de 1º de maio de 1943.** Aprova a Consolidação das Leis do Trabalho. Rio de Janeiro: Presidência da República, 1943. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del5452.htm. Acesso em: 27 out. 2026.

BRASIL. **Emenda Constitucional nº 115, de 10 de fevereiro de 2022.** Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Brasília, DF: Mesas da Câmara dos

Deputados e do Senado Federal, 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/emendas/emc/emc115.htm. Acesso em: 27 out. 2026.

BRASIL. Gabinete de Segurança Institucional da Presidência da República. **Portaria GSI/PR nº 93, de 18 de outubro de 2021.** Aprova o glossário de segurança da informação. Diário Oficial da União: seção 1, Brasília, DF, 19 out. 2021.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014.** Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Presidência da República, 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 27 out. 2026.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 27 out. 2026.

BRASIL. **Lei nº 13.853, de 8 de julho de 2019.** Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. Brasília, DF: Presidência da República, 2019. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/L13853.htm. Acesso em: 27 out. 2026.

BRASIL. **Lei nº 15.352, de 25 de fevereiro de 2026.** Transforma cargos no âmbito do Poder Executivo federal; altera a Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), para dispor sobre a Agência Nacional de Proteção de Dados (ANPD)

[...]. Conversão da Medida Provisória nº 1.317, de 2025. Brasília, DF: Presidência da República, 2026. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2026/lei/L15352.htm. Acesso em: 27 out. 2026.

BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. Secretaria de Governo Digital. **Modelo de política de gestão de registros (logs) de auditoria:** versão 2.0. Brasília, DF: SGD, mar. 2023b. Disponível em: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/modelo_politica_logs_auditoria.pdf. Acesso em: 2 nov. 2026.

BRASIL. Ministério da Saúde. Conselho Nacional de Saúde. **Resolução nº 510, de 7 de abril de 2016.** Dispõe sobre as normas aplicáveis a pesquisas em Ciências Humanas e Sociais. Diário Oficial da União: seção 1, Brasília, DF, n. 98, p. 44-46, 24 maio 2016. Disponível em: https://conselho.saude.gov.br/resolucoes/2016/Reso510.pdf. Acesso em: 2 nov. 2026.

BRASIL. Senado Federal. **Projeto de Lei nº 4.752, de 2025.** Institui o Marco Legal da Cibersegurança, cria o Programa Nacional de Segurança e Resiliência Digital e altera a Lei nº 13.756/2018. Brasília, DF: Senado Federal, 2025. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/170613. Acesso em: 2 nov. 2026.

BRASIL. Supremo Tribunal Federal (Tribunal Pleno). **Referendo na Medida Cautelar na Ação Direta de Inconstitucionalidade 6.387/DF.** Requerente: Conselho Federal da Ordem dos Advogados do Brasil. Requerido: Presidente da República. Relatora: Min. Rosa

Weber, julgado em 7 maio 2020. Diário da Justiça Eletrônico: Brasília, DF, 12 nov. 2020.

BRASIL. Tribunal Superior do Trabalho (1. Turma). **Recurso de Revista nº 613/2000-013-10-00.7.** Prova ilícita. *E-mail* corporativo. Justa causa. Divulgação de material pornográfico. Recorrente: HSBC Seguros Brasil S.A. Recorrido: Elielson Lourenço do Nascimento. Relator: Min. João Oreste Dalazen, julgado em 18 maio 2005. Diário da Justiça: Brasília, DF, 10 jun. 2005.

BRASSCOM. **Contribuição Brasscom:** tomada de subsídios: dados pessoais sensíveis - dados biométricos. Brasília, DF: Brasscom, 1 ago. 2025. Disponível em: https://brasscom.org.br/wp-content/uploads/2025/08/Brasscom-DOC-2025-046-Contribuicoes-Tomada-de-Subsidios-Dados-Biometricos_2025.08.01.pdf. Acesso em: 3 nov. 2026.

BRUNO, Fernanda. **Máquinas de ver, modos de ser:** vigilância, tecnologia e subjetividade. Porto Alegre: Sulina, 2013.

BÜCHI, Moritz; FESTIC, Noemi; LATZER, Michael. The chilling effects of digital dataveillance: a theoretical model and an empirical research agenda. **Big Data & Society,** London, v. 9, n. 1, 2022. DOI: https://doi.org/10.1177/20539517211065368.

CARDOSO, Gelson Barros; GUALBERTO, Éder Souza. **Privacidade em logs de autenticação nas IFES:** um guia técnico de conformidade com a LGPD. Brasília, DF: Universidade de Brasília, 2026. Disponível em: https://ppee.unb.br/wp-content/uploads/2026/08/Versao_Final_Privacidade_em_Logs_de_Autenticacao-1.pdf. Acesso em: 2 nov. 2026.

CARNEIRO, Maria Helena de Souza Marques. Biometria facial na administração pública: da excepcionalidade ao cotidiano. **Revista Tópicos,** Rio de Janeiro, v. 4, n. 33, p. 1-22, 2026. ISSN 2965-6672. DOI: https://doi.org/10.70773/revistatopicos/778869058.

CAVOUKIAN, Ann. **Privacy by design:** the 7 foundational principles. Toronto: Information and Privacy Commissioner of Ontario, 2009.

CHANDRAMOULI, Ramaswamy; HIBBARD, Eric. **Guidelines for media sanitization.** Gaithersburg: National Institute of Standards and Technology, 2025. (NIST Special Publication 800-88, Rev. 2). DOI: https://doi.org/10.6028/NIST.SP.800-88r2.

CICHONSKI, Paul *et al.* **Computer security incident handling guide.** Gaithersburg: National Institute of Standards and Technology, 2012. (NIST Special Publication 800-61, Rev. 2). DOI: https://doi.org/10.6028/NIST.SP.800-61r2.

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS (CNIL). **Délibération n° 2021-122 du 14 octobre 2021** portant adoption d'une recommandation relative à la journalisation. Paris: CNIL, 2021. Disponível em: https://www.cnil.fr/sites/cnil/files/atoms/files/recommandation_-_journalisation.pdf. Acesso em: 28 out. 2026.

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS (CNIL). **Délibération SAN-2023-021 du 27 décembre 2023** concernant la société Amazon France Logistique. Paris: CNIL, 2023. Disponível em: https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000048989272. Acesso em: 2 nov. 2026.

CONSELHO DA EUROPA. Corte Europeia de Direitos Humanos (Grande Câmara). **Case of Bărbulescu v. Romania.** Application no. 61496/08. Julgado em 5 set. 2017. Disponível em: https://www.echr.coe.int/w/b%C4%83rbulescu-v.-romania-no.-61496/08-. Acesso em: 28 out. 2026.

CONSELHO MONETÁRIO NACIONAL (CMN). **Resolução CMN nº 4.893, de 26 de fevereiro de 2021.** Dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições autorizadas a funcionar pelo Banco Central do Brasil. Brasília, DF: CMN, 2021. Disponível em: https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?numero=4893&tipo=RESOLU%C3%87%C3%83O+CMN. Acesso em: 28 out. 2026.

CONSELHO MONETÁRIO NACIONAL (CMN). **Resolução CMN nº 5.274, de 18 de dezembro de 2025.** Altera a Resolução CMN nº 4.893, de 26 de fevereiro de 2021. Brasília, DF: CMN, 2025. Disponível em: https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?numero=5274&tipo=RESOLU%C3%87%C3%83O+CMN. Acesso em: 28 out. 2026.

COOLEY, Thomas M. **A treatise on the law of torts or the wrongs which arise independent of contract.** 2. ed. Chicago: Callaghan, 1888.

COULL, Scott E. *et al.* Playing devil's advocate: inferring sensitive information from anonymized network traces. *In*: NETWORK AND DISTRIBUTED SYSTEM SECURITY SYMPOSIUM (NDSS), 14., 2007, San

Diego. **Proceedings** [...]. Reston: Internet Society, 2007. Disponível em: https://www.ndss-symposium.org/wp-content/uploads/2017/09/Playing-Devils-Advocate-Inferring-Sensitive-Information-from-Anonymized-Network-Traces-Scott-E.-Coull.pdf. Acesso em: 2 nov. 2026.

COX JR., Louis Anthony. What's wrong with risk matrices? **Risk Analysis,** Malden, v. 28, n. 2, p. 497-512, 2008. DOI: https://doi.org/10.1111/j.1539-6924.2008.01030.x.

DENG, Mina *et al.* A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements. **Requirements Engineering,** London, v. 16, n. 1, p. 3-32, 2011. DOI: https://doi.org/10.1007/s00766-010-0115-7.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais:** fundamentos da Lei Geral de Proteção de Dados. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

DWORKIN, Morris. **Recommendation for block cipher modes of operation:** methods for format-preserving encryption. Gaithersburg: National Institute of Standards and Technology, 2016. (NIST Special Publication 800-38G). DOI: https://doi.org/10.6028/NIST.SP.800-38G.

EASTLAKE 3RD, Donald; PANITZ, Aliza. **Reserved top level DNS names.** [*S. l.*]: Internet Engineering Task Force, 1999. (RFC 2606). DOI: https://doi.org/10.17487/RFC2606.

EUROPEAN DATA PROTECTION BOARD (EDPB). **Guidelines 01/2025 on pseudonymisation:** version 1.0, adopted for public consultation. Brussels: EDPB, 2025. Disponível em: https://www.edpb.europa.eu/our-work-tools/documents/public-

consultations/2025/guidelines-012025-pseudonymisation_en. Acesso em: 3 nov. 2026.

FRANÇA. Conseil d'État (10e et 9e chambres réunies). **Décision nº 492830:** Société Amazon France Logistique. Julgado em 23 dez. 2025. ECLI:FR:CECHR:2025:492830.20251223. Disponível em: https://www.conseil-etat.fr/fr/arianeweb/CE/decision/2025-12-23/492830. Acesso em: 3 nov. 2026.

GANTA, Srivatsava Ranjit; KASIVISWANATHAN, Shiva Prasad; SMITH, Adam. Composition attacks and auxiliary information in data privacy. *In*: ACM SIGKDD INTERNATIONAL CONFERENCE ON KNOWLEDGE DISCOVERY AND DATA MINING (KDD), 14., 2008, Las Vegas. **Proceedings** [...]. New York: ACM, 2008. p. 265-273. DOI: https://doi.org/10.1145/1401890.1401926.

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI. **Provvedimento n. 364 del 6 giugno 2024:** documento di indirizzo "Programmi e servizi informatici di gestione della posta elettronica nel contesto lavorativo e trattamento dei metadati". Roma: Garante, 2024. Disponível em: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/10026277. Acesso em: 28 out. 2026.

GIL, Antonio Carlos. **Como elaborar projetos de pesquisa.** 6. ed. São Paulo: Atlas, 2017.

GREGOR, Shirley; HEVNER, Alan R. Positioning and presenting design science research for maximum impact. **MIS Quarterly,** Minneapolis, v. 37, n. 2, p. 337-355, 2013. DOI: https://doi.org/10.25300/MISQ/2013/37.2.01.

HERNANDEZ-RAMOS, Jose Luis *et al.* Intrusion detection based on federated learning: a systematic review. **ACM Computing Surveys,** New York, v. 57, n. 12, p. 1-65, 2025. DOI: https://doi.org/10.1145/3731596.

HEVNER, Alan R. *et al.* Design science in information systems research. **MIS Quarterly,** Minneapolis, v. 28, n. 1, p. 75-105, 2004. DOI: https://doi.org/10.2307/25148625.

HOEPMAN, Jaap-Henk. Privacy design strategies. *In*: IFIP INTERNATIONAL INFORMATION SECURITY CONFERENCE (SEC), 29., 2014, Marrakech. **ICT systems security and privacy protection.** Berlin: Springer, 2014. p. 446-459. DOI: https://doi.org/10.1007/978-3-642-55415-5_38.

INFORMATION COMMISSIONER'S OFFICE (ICO). **Employment practices and data protection:** monitoring workers. Wilmslow: ICO, 2023. Disponível em: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/employment/monitoring-workers/. Acesso em: 28 out. 2026.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). **ISO/IEC 27000:2018:** information technology - security techniques - information security management systems – overview and vocabulary. 5. ed. Geneva: ISO, 2018.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). **ISO/IEC 27005:2022:** information security, cybersecurity and privacy protection - guidance on managing information security risks. 4. ed. Geneva: ISO, 2022.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). **ISO/IEC 27701:2025:** information security, cybersecurity and privacy

protection - privacy information management systems - requirements and guidance. 2. ed. Geneva: ISO, 2025.

JI, Ziwei *et al.* Survey of hallucination in natural language generation. **ACM Computing Surveys,** New York, v. 55, n. 12, art. 248, p. 1-38, 2023. DOI: https://doi.org/10.1145/3571730.

KENT, Alexander D. **Comprehensive, multi-source cyber-security events data set.** Los Alamos: Los Alamos National Laboratory, 2015. DOI: https://doi.org/10.17021/1179829.

KENT, Karen; SOUPPAYA, Murugiah. **Guide to computer security log management.** Gaithersburg: National Institute of Standards and Technology, 2006. (NIST Special Publication 800-92). DOI: https://doi.org/10.6028/NIST.SP.800-92.

KOOPS, Bert-Jaap; LEENES, Ronald. Privacy regulation cannot be hardcoded: a critical comment on the 'privacy by design' provision in data-protection law. **International Review of Law, Computers & Technology,** Abingdon, v. 28, n. 2, p. 159-171, 2014. DOI: https://doi.org/10.1080/13600869.2013.801589.

LINDAUER, Brian. **Insider threat test dataset.** Pittsburgh: Carnegie Mellon University, 2020. DOI: https://doi.org/10.1184/R1/12841247.v1.

MANDIANT. **M-Trends 2026:** data, insights, and strategies from the frontlines. [*S. l.*]: Google Cloud, 23 mar. 2026. Disponível em: https://cloud.google.com/blog/topics/threat-intelligence/m-trends-2026. Acesso em: 2 nov. 2026.

MCKAY, Kerry; COOPER, David. **Guidelines for the selection, configuration, and use of Transport Layer Security (TLS)**

implementations. Gaithersburg: National Institute of Standards and Technology, 2019. (NIST Special Publication 800-52, Rev. 2). DOI: https://doi.org/10.6028/NIST.SP.800-52r2.

MENDES, Laura Schertel; MATTIUZZO, Marcela. Discriminação algorítmica: conceito, fundamento legal e tipologia. **Direito Público,** Porto Alegre, v. 16, n. 90, p. 39-64, nov./dez. 2019. Disponível em: https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/3766. Acesso em: 27 out. 2026.

MENDES, Laura Schertel; RODRIGUES JÚNIOR, Otavio Luiz; FONSECA, Gabriel Campos Soares da. O Supremo Tribunal Federal e a proteção constitucional dos dados pessoais: rumo a um direito fundamental autônomo. *In*: DONEDA, Danilo *et al.* (coord.). **Tratado de proteção de dados pessoais.** Rio de Janeiro: Forense, 2021. p. 61-71.

MENGES, Florian *et al.* Towards GDPR-compliant data processing in modern SIEM systems. **Computers & Security,** Amsterdam, v. 103, 102165, 2021. DOI: https://doi.org/10.1016/j.cose.2020.102165.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). **The keyed-hash message authentication code (HMAC).** Gaithersburg: NIST, 2008. (Federal Information Processing Standards Publication 198-1). DOI: https://doi.org/10.6028/NIST.FIPS.198-1.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). **The NIST Cybersecurity Framework (CSF) 2.0.** Gaithersburg: NIST, 2024. DOI: https://doi.org/10.6028/NIST.CSWP.29.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). **The NIST Privacy Framework:** a tool for improving privacy through

enterprise risk management, version 1.0. Gaithersburg: NIST, 2020. DOI: https://doi.org/10.6028/NIST.CSWP.01162020.

NELSON, Alex *et al.* **Incident response recommendations and considerations for cybersecurity risk management:** a CSF 2.0 community profile. Gaithersburg: National Institute of Standards and Technology, 2025. (NIST Special Publication 800-61, Rev. 3). DOI: https://doi.org/10.6028/NIST.SP.800-61r3.

NISSENBAUM, Helen. Privacy as contextual integrity. **Washington Law Review,** Seattle, v. 79, n. 1, p. 119-157, 2004. Disponível em: https://digitalcommons.law.uw.edu/wlr/vol79/iss1/10. Acesso em: 2 nov. 2026.

OLIVEIRA NETO, Célio Pereira. Proteção de dados e uso da tecnologia no monitoramento do trabalhador: da experiência portuguesa às projeções no Brasil. **Revista Electrónica de Direito,** Porto, v. 31, n. 2, p. 169-209, 2023. DOI: https://doi.org/10.24840/2182-9845_2023-0002_0007.

OLIVEIRA, Lourival José de; SILVA, Fabiano Fernando da. Biometria facial e tecnologias de monitoramento à luz dos direitos da personalidade do trabalhador: aspectos do capitalismo de vigilância e da sociedade do controle nas relações laborais. **Revista da Faculdade de Direito da UFMG,** Belo Horizonte, n. 84, p. 265-284, jan./jun. 2024. DOI: https://doi.org/10.12818/P.0304-2340.2024v84p265.

PARASURAMAN, Raja; MANZEY, Dietrich H. Complacency and bias in human use of automation: an attentional integration. **Human Factors,** Thousand Oaks, v. 52, n. 3, p. 381-410, 2010. DOI: https://doi.org/10.1177/0018720810376055.

PCI SECURITY STANDARDS COUNCIL. **Payment Card Industry Data Security Standard:** requirements and testing procedures, version 4.0.1. Wakefield: PCI SSC, 2024. Disponível em: https://www.pcisecuritystandards.org/document_library/. Acesso em: 28 out. 2026.

PEFFERS, Ken *et al.* A design science research methodology for information systems research. **Journal of Management Information Systems,** Armonk, v. 24, n. 3, p. 45-77, 2007. DOI: https://doi.org/10.2753/MIS0742-1222240302.

PENNEY, Jonathon W. Chilling effects: online surveillance and Wikipedia use. **Berkeley Technology Law Journal,** Berkeley, v. 31, n. 1, p. 117-182, 2016. DOI: https://doi.org/10.15779/Z38SS13.

RESENDE, Haydgi Oliveira; PORTES FILHO, João Luis de Oliveira; SANTOS FILHO, Victor Amato dos. Automação da anonimização de dados pessoais em pipelines de ETL com Python: uma abordagem orientada à conformidade com a LGPD. **Revista Tópicos,** Rio de Janeiro, v. 4, n. 33, p. 1-17, 2026. ISSN 2965-6672. DOI: https://doi.org/10.70773/revistatopicos/779337016.

ROBLES-GONZÁLEZ, Antonio; PARRA-ARNAU, Javier; FORNÉ, Jordi. A LINDDUN-based framework for privacy threat analysis on identification and authentication processes. **Computers & Security,** Amsterdam, v. 94, 101755, 2020. DOI: https://doi.org/10.1016/j.cose.2020.101755.

RODOTÀ, Stefano. **A vida na sociedade da vigilância:** a privacidade hoje. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

SHOSTACK, Adam. **Threat modeling:** designing for security. Indianapolis: Wiley, 2014.

SION, Laurens *et al.* Robust and reusable LINDDUN privacy threat knowledge. **Computers & Security,** Amsterdam, v. 154, 104419, 2025. DOI: https://doi.org/10.1016/j.cose.2025.104419.

SOLOVE, Daniel J. A taxonomy of privacy. **University of Pennsylvania Law Review,** Philadelphia, v. 154, n. 3, p. 477-564, 2006. DOI: https://doi.org/10.2307/40041279.

SOLOVE, Daniel J. **Nothing to hide:** the false tradeoff between privacy and security. New Haven: Yale University Press, 2011.

SPIEKERMANN, Sarah; CRANOR, Lorrie Faith. Engineering privacy. **IEEE Transactions on Software Engineering,** New York, v. 35, n. 1, p. 67-82, 2009. DOI: https://doi.org/10.1109/TSE.2008.88.

SWEENEY, Latanya. k-anonymity: a model for protecting privacy. **International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems,** Singapore, v. 10, n. 5, p. 557-570, 2002. DOI: https://doi.org/10.1142/S0218488502001648.

UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.** Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (Regulamento Geral sobre a Proteção de Dados). Jornal Oficial da União Europeia: série L, Luxemburgo, n. 119, p. 1-88, 4 maio 2016a. Disponível em: https://eur-lex.europa.eu/eli/reg/2016/679/oj. Acesso em: 28 out. 2026.

UNIÃO EUROPEIA. **Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho, de 13 de junho de 2024.** Cria regras harmonizadas em matéria de inteligência artificial (Regulamento da Inteligência Artificial). Jornal Oficial da União Europeia: série L, Luxemburgo, 12 jul. 2024. Disponível em: https://eur-lex.europa.eu/eli/reg/2024/1689/oj. Acesso em: 28 out. 2026.

UNIÃO EUROPEIA. **Regulamento (UE) 2026/1744 do Parlamento Europeu e do Conselho, de 8 de julho de 2026.** Altera os Regulamentos (UE) 2024/1689, (UE) 2018/1139 e (UE) 2023/1230 no que diz respeito à simplificação da aplicação de regras harmonizadas em matéria de inteligência artificial (Omnibus Digital sobre IA). Jornal Oficial da União Europeia: série L, Luxemburgo, 24 jul. 2026. Disponível em: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=oj%3AL_202601744. Acesso em: 28 out. 2026.

UNIÃO EUROPEIA. Tribunal de Justiça (Primeira Secção). **Processo C-413/23 P:** European Data Protection Supervisor (EDPS) contra Single Resolution Board (SRB). Julgado em 4 set. 2025. ECLI:EU:C:2025:645. Disponível em: https://curia.europa.eu/juris/documents.jsf?num=C-413/23%20P. Acesso em: 2 nov. 2026.

UNIÃO EUROPEIA. Tribunal de Justiça (Segunda Secção). **Processo C-582/14:** Patrick Breyer contra Bundesrepublik Deutschland. Julgado em 19 out. 2016b. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:62014CJ0582. Acesso em: 28 out. 2026.

VENABLE, John; PRIES-HEJE, Jan; BASKERVILLE, Richard. FEDS: a framework for evaluation in design science research. **European**

Journal of Information Systems, Abingdon, v. 25, n. 1, p. 77-89, 2016. DOI: https://doi.org/10.1057/ejis.2014.36.

WACHTER, Sandra; MITTELSTADT, Brent; FLORIDI, Luciano. Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation. **International Data Privacy Law,** Oxford, v. 7, n. 2, p. 76-99, 2017. DOI: https://doi.org/10.1093/idpl/ipx005.

WARREN, Samuel D.; BRANDEIS, Louis D. The right to privacy. **Harvard Law Review,** Cambridge, v. 4, n. 5, p. 193-220, 1890. DOI: https://doi.org/10.2307/1321160.

XU, Jun *et al.* Prefix-preserving IP address anonymization: measurement-based security evaluation and a new cryptography-based scheme. *In*: IEEE INTERNATIONAL CONFERENCE ON NETWORK PROTOCOLS (ICNP), 10., 2002, Paris. **Proceedings** [...]. Los Alamitos: IEEE Computer Society, 2002. p. 280-289. DOI: https://doi.org/10.1109/ICNP.2002.1181415.

ZUBOFF, Shoshana. **A era do capitalismo de vigilância:** a luta por um futuro humano na nova fronteira do poder. Tradução de George Schlesinger. Rio de Janeiro: Intrínseca, 2020.

GLOSSÁRIO

AES-256-GCM. Cifra simétrica *Advanced Encryption Standard* com chave de 256 bits no modo *Galois/Counter*, que protege o sigilo e a integridade dos dados armazenados.

Anonimização. A LGPD a define como “utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo” (Brasil, 2018, art. 5º, XI).

Artefato. Documento que cada passo do *framework* produz e que o controlador aprova e mantém versionado, como o registro de casos de uso ou o dicionário de dados (Quadro 7). Registra a decisão tomada e integra a evidência de auditoria.

Cadeia de custódia. Procedimentos que documentam a identificação, a coleta, a guarda e o manuseio de evidências digitais, para preservar sua integridade e seu valor probatório (ABNT, 2013).

Controlador. A LGPD o define como “pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais” (Brasil, 2018, art. 5º, VI).

Crypto-PAn. Esquema criptográfico de anonimização de endereços IP com preservação de prefixo. Endereços que compartilham os primeiros bits continuam a compartilhá-los após a cifra, o que mantém as relações de sub-rede, e a transformação pode ser invertida com a chave (Xu *et al.*, 2002).

DLP (*Data Loss Prevention*). Ferramenta que inspeciona mensagens, arquivos e transferências para impedir o vazamento de informação classificada.

EDR (*Endpoint Detection and Response*). Ferramenta instalada em estações e servidores que registra processos, arquivos e conexões para detectar ataques e responder a eles no próprio dispositivo.

Encarregado. Quem o controlador e o operador indicam para intermediar a comunicação com os titulares e com a ANPD (Brasil, 2018, art. 5º, VIII; ANPD, 2024c).

Evidência de auditoria. Conjunto formado pelos artefatos e pela trilha de auditoria, que permite a um terceiro verificar se as decisões do *framework* foram tomadas e cumpridas.

HMAC (*keyed-hash message authentication code*). Código de autenticação de mensagem calculado com função de *hash* e chave secreta (NIST, 2008). Usado como pseudônimo, não revela o identificador a quem não detém a chave.

HSM (*Hardware Security Module*). Dispositivo físico que gera, guarda e usa chaves criptográficas sem expô-las ao sistema hospedeiro.

Indicador de auditoria. Medida calculada sobre um artefato ou sobre a trilha de auditoria, com fórmula, meta e periodicidade (Quadro 8), que mostra se a decisão registrada continua a ser cumprida.

IoC (*Indicator of Compromise*). Artefato observável, como endereço, domínio ou *hash* de arquivo, que indica atividade maliciosa.

***k*-anonimato.** Propriedade de um conjunto de dados em que cada registro é indistinguível de pelo menos *k* - 1 outros quanto aos atributos que poderiam identificá-lo (Sweeney, 2002).

LINDDUN. Taxonomia de ameaças à privacidade (Deng *et al.*, 2011; Sion *et al.*, 2025), com sete categorias: *Linking* (associar dados ou ações para saber mais sobre uma pessoa ou grupo); *Identifying*

(descobrir a identidade de uma pessoa); *Non-repudiation* (poder atribuir uma ação ou declaração a uma pessoa); *Detecting* (deduzir, por observação, o envolvimento de uma pessoa); *Data Disclosure* (coletar, armazenar, tratar ou compartilhar dados pessoais em excesso); *Unawareness and Unintervenability* (informar ou envolver insuficientemente os titulares, que não conseguem intervir no tratamento); e *Non-compliance* (desviar-se de normas, boas práticas e legislação de proteção de dados). Diferentemente das categorias do STRIDE, voltadas aos sistemas, as do LINDDUN tratam de ameaças aos titulares.

NetFlow/IPFIX. Formatos de exportação de registros de fluxos de rede, com origem, destino, portas, volume e horário, sem o conteúdo das comunicações. IPFIX significa *IP Flow Information Export*.

Operador. A LGPD o define como "pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador" (Brasil, 2018, art. 5º, VII).

PAM (*Privileged Access Management*). Solução de gestão de acesso privilegiado que guarda em cofre as credenciais das contas administrativas, libera-as por sessão e registra seu uso.

Pseudonimização. A LGPD a define como:

> *tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro (Brasil, 2018, art. 13, § 4º).*

RBAC (*Role-Based Access Control*). Controle de acesso em que as permissões se vinculam a papéis, aos quais os usuários são associados.

Registro das operações. Registro das operações de tratamento que o controlador e o operador devem manter (Brasil, 2018, art. 37). No *framework*, é alimentado pelo registro de casos de uso do Passo 1.

SIEM (*Security Information and Event Management*). Plataforma que coleta, normaliza e correlaciona registros de várias fontes para detectar incidentes.

SOC (*Security Operations Center*). Equipe e infraestrutura que monitoram o ambiente de forma contínua, detectam incidentes e respondem a eles.

STRIDE. Taxonomia de ameaças à segurança (Shostack, 2014), com seis categorias: *Spoofing* (falsificar uma identidade); *Tampering* (adulterar dados ou código); *Repudiation* (negar ter praticado uma ação); *Information Disclosure* (expor informação a quem não deveria acessá-la); *Denial of Service* (negar ou degradar o serviço); e *Elevation of Privilege* (obter privilégios não autorizados).

TEE (*Trusted Execution Environment*). Área isolada do processador que executa código e guarda dados protegidos do sistema operacional hospedeiro.

Telemetria. Registros gerados automaticamente por sistemas e dispositivos, como *logs*, eventos, fluxos de rede e consultas ao sistema de nomes de domínio (DNS), usados no monitoramento. No texto, “registros”, no plural e sem qualificação, designa esses dados.

TLS (*Transport Layer Security*). Protocolo que cifra e autentica comunicações em trânsito.

Trilha de auditoria. Registro cronológico e protegido contra alteração das ações realizadas em um sistema, que permite reconstituir quem fez o quê e quando. No *framework*, abrange as consultas e reidentificações do SOC (Passo 6).

UEBA (*User and Entity Behavior Analytics*). Análise do comportamento de usuários e dispositivos que aponta desvios em relação a um perfil de referência.

Viés de automação. Tendência de aceitar, sem verificação suficiente, as saídas de um sistema automatizado, associada à complacência do operador humano (Parasuraman; Manzey, 2010).

APÊNDICE A - PROTOCOLO DE SELEÇÃO DO *CORPUS* E LIVRO DE CÓDIGOS

Quadro 5. Protocolo de seleção e codificação das fontes

Elemento	Descrição
Repositórios de fontes primárias	Presidência da República, Diário Oficial da União, Câmara dos Deputados, Senado Federal, ANPD, STF, TST, CMN, NIST, ISO, ABNT, EDPB, CNIL, Garante italiano e tribunais estrangeiros citados.
Buscas dirigidas	Google Scholar e portais de editores, com termos sobre proteção de dados (LGPD, RGPD), monitoramento de segurança (SIEM, SOC, UEBA, EDR, DLP) e engenharia de privacidade (pseudonimização, LINDDUN), além de busca complementar sobre detecção com preservação de privacidade, ameaça interna e monitoramento do empregado após a LGPD.
Idiomas	Termos de busca em português e inglês. Fontes primárias estrangeiras lidas nos idiomas originais (francês, italiano e alemão).
Rastreamento de citações	A partir de obras seminais citadas nas fontes selecionadas.
Período e data de corte	Sem recorte temporal, com data de corte em 3 nov. 2026, após a qual atos e publicações não foram considerados.
Inclusão	Fontes primárias vigentes, ou revogadas quando relevantes, e literatura revisada por pares ou de referência.
Exclusão	Materiais promocionais e textos sem lastro normativo ou empírico.
Registro das buscas	Seleção intencional, sem registro do número de resultados brutos por busca, o que impede reproduzi-la com exatidão.

Codificação	Dedutiva, por um pesquisador, com as categorias prévias do Quadro 6, que abrangem os princípios do art. 6º da LGPD, STRIDE, LINDDUN, relação entre pares, graus do regulamento de dosimetria e notas P e I do índice.
Composição do *corpus*	120 fontes, distribuídas entre 11 atos normativos nacionais e projetos de lei; 13 atos, orientações e relatórios da ANPD, do CMN e do BCB; 10 decisões administrativas e judiciais; 6 orientações de autoridades estrangeiras; 3 atos normativos da União Europeia (os acórdãos do seu Tribunal de Justiça contam entre as decisões); 23 normas, publicações técnicas e bases de dados; 33 artigos em periódicos revisados por pares (16 a partir de 2017); 5 trabalhos em eventos; 16 livros, capítulos, relatórios e trabalhos acadêmicos. A Resolução nº 510/2016 do Conselho Nacional de Saúde, citada apenas nos aspectos éticos (Seção 3.2), não integra o *corpus*.
Suficiência	Analítica. O levantamento foi dado por concluído quando os sete cenários do Quadro 1, os cinco elementos do *pipeline* e todas as categorias do Quadro 6 passaram a apoiar-se em ao menos uma fonte primária.
Atualização (protocolo prospectivo)	Cada atualização registra base, expressão de busca, data, resultados recuperados, exclusões por critério e fontes incluídas. As duplicatas são removidas pelo DOI ou, na falta dele, por título, autoria e ano, e um segundo pesquisador recodifica às cegas uma amostra da matriz, com medida de concordância entre avaliadores.

Fonte: Elaborado pelos autores (2026).

Quadro 6. Livro de códigos: categoria, definição operacional e regra de decisão

Categoria	Definição operacional	Regra de decisão e exemplo

Convergência	O controle de segurança também reduz a ameaça de privacidade do par.	O controle não acrescenta dados, vínculos nem identificação, como o TLS mútuo, que reduz *Data Disclosure* na ingestão.
Tensão	O controle aumenta a ameaça de privacidade, mas há controle de conciliação que satisfaz ambos.	Exige nomear o controle de conciliação. É o caso da correlação por conta, de que depende a detecção de *Spoofing*, conciliada por pseudônimo determinístico e cofre.
Conflito	Nenhum dos controles examinados satisfaz ambos os objetivos no mesmo escopo.	Na dúvida entre tensão e conflito, o par é classificado como conflito e o escopo é delimitado. Exemplo disso é o não repúdio de ações privadas, pois nenhum dos controles examinados assegura a atribuição e a negabilidade da mesma ação.
P = 1	A prática exige configuração atípica para existir.	Recurso desativado por padrão ou dependente de módulo adicional.
P = 2	A prática depende de decisão de política da organização.	Exige finalidade, regra ou escopo definidos por alguém, como no reuso de *logs* para avaliação.
P = 3	A prática ocorre por omissão.	Comportamento padrão da ferramenta, como a retenção sem expurgo.
I = 1	Impacto limitado sobre os titulares.	Sem dado sensível nem efeito sobre o emprego, com salvaguardas aplicadas.
I = 2	Pode afetar significativamente interesses e direitos, sem agravante.	Dado pessoal identificável usado fora das salvaguardas, sem as hipóteses de I = 3.
I = 3	Há agravante, como dado sensível, larga	O agravante que justifica a nota fica registrado. Na dúvida entre 2 e

	escala ou efeito discriminatório, ou efeito direto sobre o emprego ou a vida privada.	3, ambas são testadas na análise de sensibilidade (Apêndice C).

Fonte: Elaborado pelos autores (2026), com base em Deng *et al.* (2011), Shostack (2014) e ANPD (2023a).

APÊNDICE B - ARTEFATOS, ESPECIFICAÇÃO TÉCNICA E EXEMPLO DE APLICAÇÃO

Quadro 7. Artefatos por passo: conteúdo mínimo, responsáveis e gatilhos de revisão

Passo e artefato	Conteúdo mínimo	Responsáveis	Gatilhos de revisão
1 Registro de casos de uso	Fonte de telemetria, ameaça a detectar, regra do SIEM, campos usados e responsável.	Segurança elabora e gestor do SOC aprova, após consulta ao encarregado.	Nova fonte ou regra, ou fonte sem caso de uso.
2 Registro de hipótese legal e teste de balanceamento	Operação, hipótese legal, finalidade, necessidade, expectativa do titular e salvaguardas, além da análise de alto risco e do RIPD, quando cabível.	Jurídico e Privacidade elaboram e controlador aprova, após consulta ao encarregado.	Nova finalidade, dado sensível ou nova categoria de titular.

3 Dicionário de dados e tabela de temporalidade	Campo, fonte, necessidade, tratamento (manter, agregar, pseudonimizar ou suprimir, conforme a Figura 2), prazo e forma de descarte.	Segurança e TI elaboram e controlador aprova, após consulta ao encarregado.	Mudança de regra de detecção, de obrigação setorial ou de fornecedor.
4 Especificação de salvaguardas e ficha de pseudonimização	Técnica por campo, gestão e rotação de chaves, HSM (ou serviço gerenciado de chaves) e cofre, papéis de acesso, acesso emergencial e fluxo de reidentificação.	TI e Segurança elaboram e controlador aprova.	Rotação de chave, incidente ou novo perfil de acesso.
5 Aviso interno e canal de contestação	Categorias coletadas, finalidades, prazos, existência de escores, direitos, canal e prazo de resposta (modelo no Quadro 11).	Jurídico, Privacidade e Recursos Humanos elaboram, controlador aprova e divulga, e encarregado recebe as contestações.	Mudança nos Passos 1 a 4 ou contestações recorrentes.
6 Trilha de auditoria, relatório de reidentificações e RIPD versionado	Consultas e reidentificações com autor, justificativa, aprovação e data, indicadores de auditoria do Quadro 3 e	Segurança gera a trilha. O encarregado recebe o relatório, emite parecer e pode recomendar ajustes, e o	Periodicidade definida (por exemplo, trimestral), desvio de indicador de auditoria ou mudança de regra, fonte ou

	histórico de versões do RIPD.	controlador aprova cada versão do RIPD.	fornecedor, que gera nova versão do RIPD.

Fonte: Elaborado pelos autores (2026). Cada linha corresponde a uma evidência de auditoria e pode servir de lista de verificação para o encarregado ou o gestor de SOC. As fórmulas dos indicadores de auditoria estão no Quadro 8.

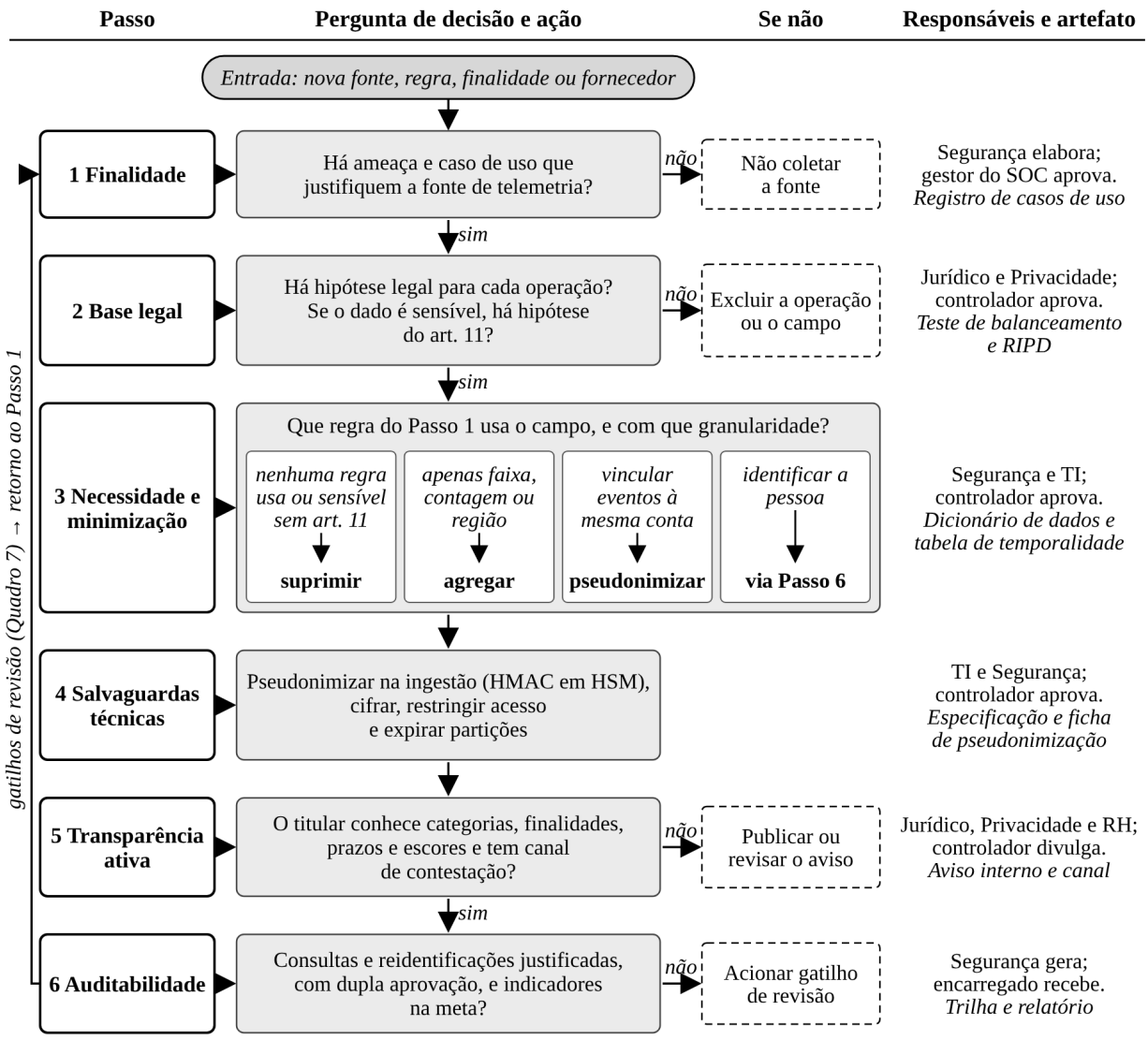
Quadro 8. Indicadores de auditoria: fórmula, meta ilustrativa e periodicidade

Passo	Indicador e fórmula	Meta ilustrativa	Periodicidade
1 Finalidade	Fontes sem caso de uso ÷ fontes de telemetria ativas.	0%	Trimestral e a cada nova fonte
2 Base legal	Operações sem hipótese documentada ÷ operações do registro.	0%	Semestral e a cada nova finalidade
3 Necessidade e minimização	(a) Média de campos pessoais por tipo de evento. (b) Idade do registro mais antigo ÷ prazo da tabela de temporalidade. (c) Unidades com menos de *k* contas ativas não agregadas por região.	(a) Queda ante a linha de base, (b) razão ≤ 1 e (c) zero	Mensal
4 Salvaguardas técnicas	(a) Campos identificadores pseudonimizados na ingestão ÷ campos identificadores do dicionário. (b) Acessos	100% em (a) e (b)	Trimestral

	privilegiados revisados ÷ concedidos.		
5 Transparência ativa	Contestações respondidas no prazo ÷ recebidas, com o prazo do art. 19, II, da LGPD como referência.	100%	Trimestral
6 Auditabilidade	Reidentificações com justificativa e dupla aprovação ÷ reidentificações.	100%	Trimestral, no relatório ao encarregado

Fonte: Elaborado pelos autores (2026). Metas a calibrar por organização. O desvio da meta aciona os gatilhos de revisão do Quadro 7.

Figura 2. Fluxo de decisão do *framework*: perguntas, saídas, responsáveis e retorno



Fonte: Elaborada pelos autores (2026).

A especificação técnica a seguir detalha, para organizações de grande porte, as salvaguardas dos Passos 3 e 4 resumidas na Seção 5.2. Como HSM, ambientes de execução confiáveis e cofre de *tokens* elevam o custo e a latência da operação, o perfil reduzido do Apêndice D, para agentes de pequeno porte, troca o HSM e esses ambientes por chaves controladas pelo cliente em serviço gerenciado de nuvem e por segredos efêmeros em memória nos coletores. Nos repositórios imutáveis, o expurgo em camadas atribui a cada partição temporal uma chave própria, destruída ao fim do prazo (apagamento criptográfico). Como a destruição da chave torna inacessíveis apenas as cópias cifradas com ela, réplicas, cópias de segurança e índices derivados precisam seguir o mesmo ciclo.

Partições sob preservação judicial ficam fora do expurgo até o fim do processo.

A pseudonimização do identificador obedece a um fluxo em que o identificador é normalizado, o HMAC é calculado no HSM e somente o pseudônimo é armazenado, enquanto a correspondência fica em cofre separado, com registro de cada reidentificação autorizada. Como o HMAC não oferece operação de reversão, a reidentificação autorizada depende do cofre ou da substituição do HMAC por uma cifra que preserva o formato, reversível com a chave (Dworkin, 2016). O pseudônimo armazenado mantém comprimento suficiente para que colisões sejam desprezíveis, já que o truncamento excessivo, como o da forma abreviada do Quadro 4, eleva essa probabilidade. Resta, porém, o risco de que quem detém a chave reidentifique os titulares por enumeração, pois o espaço de identificadores corporativos é pequeno. A chave raiz permanece no HSM, com escopo por domínio e rotação periódica, e cada reidentificação exige separação de funções e controle duplo.

Em *pipelines* de alta vazão, em que consultar o HSM a cada evento acrescentaria latência excessiva, o HSM deriva chaves operacionais por domínio, que nunca saem da memória de ambientes de execução confiáveis (TEE) nos coletores. As chaves operacionais são rotacionadas no ritmo da linha de base comportamental, para não romper a vinculação de eventos da mesma conta. Identificadores que aparecem em campos livres, como caminhos de diretório e linhas de comando, são higienizados por expressões regulares antes da indexação. Para o endereço IP, a especificação adota a Crypto-PAn, bijetiva e invertível com a chave, que, diferentemente da cifra que preserva apenas o formato, mantém as relações de sub-rede. Como a preservação das sub-redes permite inferir a topologia, a

chave do esquema recebe o mesmo controle de acesso aplicado ao cofre.

Na agregação geográfica, o limiar adotado é de $k = 10$ contas ativas, abaixo do qual a unidade federativa é agregada por região. A chance de associar um evento a uma conta somente pela unidade fica limitada a $1/k$, embora o horário e o volume elevem esse risco. Cada organização calibra k no RIPD mediante a ponderação entre esse risco e a perda do sinal de deslocamento, e o indicador de auditoria do Passo 3 verifica mensalmente as unidades abaixo do limiar. No teletrabalho, porém, horários de jornada repetidos permitem isolar a conta pela interseção de visões sucessivas, mesmo com $k \geq 10$. Para neutralizar esse ataque, as visões de tendência do UEBA agrupam os horários em intervalos de 15 ou 30 minutos, e o horário exato fica restrito às regras de detecção e à camada cifrada de resposta a incidentes.

Os Quadros 9 a 11 aplicam essa especificação ao cenário bancário. Cada operação é rastreada, no primeiro, até a hipótese legal e, quando houver, até a norma setorial ou regulamentar que a impõe, com os dados tratados e a salvaguarda correspondente. O segundo acompanha um alerta de UEBA do disparo ao expurgo e indica, em cada etapa, o dado tratado, quem autoriza, o prazo e o evento de revisão. Por fim, o modelo de aviso interno do Passo 5 informa categorias, finalidades, prazos, existência de escores e canal de contestação, sem revelar as regras de detecção.

Quadro 9. Rastreabilidade das operações no cenário bancário: dados, hipótese legal, norma e salvaguarda

Operação	Dados tratados	Hipótese legal	Norma setorial ou regulamentar	Salvaguarda
Autenticação e trilhas de auditoria de acesso	Pseudônimo, IP cifrado, horário e resultado	Obrigação regulatória (art. 7º, II)	Res. CMN nº 4.893/2021, art. 3º, §§ 2º e 7º	Retenção por tipo de processamento e RBAC
Detecção de intrusão em rede e estações	Eventos de processo e conexão, com IP cifrado	Obrigação regulatória (art. 7º, II)	Res. CMN nº 4.893/2021, art. 3º, § 2º	Apenas eventos de segurança, sem conteúdo
Prevenção de vazamento de dados classificados	Volume de saída e *hash* de arquivo classificado	Obrigação regulatória, restrita ao controle exigido	Res. CMN nº 4.893/2021, art. 3º, § 2º	Somente padrões classificados, sem conteúdo de mensagens
Análise comportamental de contas (UEBA)	Pseudônimo, unidade federativa, horário agrupado em intervalos e volume	Legítimo interesse (arts. 7º, IX, e 10)	Nenhuma, pois excede o rol do art. 3º, § 2º	Teste de balanceamento, RIPD, aviso e revisão humana
Autenticação por dinâmica de digitação	Ritmo de digitação comparado ao perfil da conta	Nenhuma hipótese do art. 11 (tese adotada)	Nenhuma	Supressão no Passo 2

Preservação de evidências de incidente	Registros vinculados ao incidente	Exercício regular de direitos (art. 7º, VI), se apto a gerar processo	Res. CD/ANPD nº 15/2024 (registro do incidente)	Cadeia de custódia e exclusão do expurgo até o fim do processo

Fonte: Elaborado pelos autores (2026), com base em Brasil (2018), Conselho Monetário Nacional (2021, 2025), ANPD (2024b) e ABNT (2013). Cenário hipotético.

Quadro 10. Exemplo ponta a ponta: do alerta de UEBA ao expurgo, no cenário bancário

Etapa	Dados e tratamento	Responsável e autorização	Prazo, registro e revisão
1 Alerta	Volume anômalo de saída na conta usr_9f8a7b6c, a partir de IP cifrado e unidade federativa incomum, sem nenhum identificador direto.	Regra do Passo 1, sem decisão automática sobre a conta.	Alerta e consulta registrados na trilha de auditoria (Passo 6).
2 Triagem	Consulta, sob pseudônimo, aos eventos da conta nos últimos 30 dias. O destino é confrontado com listas de reputação enriquecidas na ingestão.	Analista do SOC, com perfil RBAC de triagem.	Consulta registrada com justificativa. Eventual resumo gerado por IA é conferido contra os eventos de origem.
3 Pedido de reidentificação	Com o indício confirmado (destino em lista de reputação), o	Gestor do SOC e responsável por Privacidade aprovam	Justificativa, aprovadores e horário ficam no cofre e entram

	analista pede a identidade do titular da conta.	(controle duplo), e o encarregado é informado.	no relatório trimestral ao encarregado.
4 Resposta	Contenção da conta e preservação seletiva dos registros do incidente sob cadeia de custódia (ABNT, 2013).	Equipe de resposta a incidentes, com avaliação do Jurídico sobre a comunicação à ANPD e aos titulares.	Comunicação em três dias úteis, se houver risco ou dano relevante, e registro do incidente por cinco anos (ANPD, 2024b).
5 Expurgo	Telemetria sem IoC expurgada aos seis meses, e registros preservados fora do expurgo até o fim do processo. Conteúdo e dinâmica de digitação nunca foram coletados.	Automático, conforme a tabela de temporalidade do Passo 3.	Indicador de retenção efetiva (Quadro 8) e exceções justificadas.
6 Revisão	Ajuste de regra, de campo ou de prazo a partir das lições do incidente.	Segurança propõe, encarregado emite parecer e controlador aprova.	Nova versão do RIPD e do dicionário de dados, se houver mudança.

Fonte: Elaborado pelos autores (2026). Cenário hipotético, com prazos ilustrativos.

Quadro 11. Modelo de aviso interno aos colaboradores (Passo 5)

Monitoramento de segurança da informação. A [instituição] monitora seus sistemas corporativos para detectar acessos indevidos, credenciais comprometidas e vazamento de dados classificados. São tratados, sob pseudônimo, registros de autenticação, conexões de rede, eventos de

segurança das estações e volumes de transferência. Não são coletados o conteúdo de mensagens nem o ritmo de digitação. Alertas automáticos orientam a equipe de segurança e não geram, sozinhos, bloqueio definitivo ou sanção, pois toda medida passa por revisão humana. Os dados não são usados para avaliar produtividade. Registros sem indício de incidente são eliminados em [prazo], e os de incidentes são preservados pelo tempo necessário à apuração. Dúvidas, pedidos de acesso e contestações podem ser enviados ao encarregado pelo canal [canal], com resposta em até [prazo]. As regras de detecção são confidenciais, por razões de segurança.

Fonte: Elaborado pelos autores (2026). Os campos entre colchetes são preenchidos por cada organização.

APÊNDICE C - POSICIONAMENTO, AVALIAÇÃO *EX ANTE* E ÍNDICE DE PRIORIZAÇÃO

Os estudos acadêmicos mais próximos são comparados no Quadro 12 quanto a objeto, base normativa e lacuna, e os referenciais de gestão e de mercado, no Quadro 13. Neste último, as colunas de ancoragem na LGPD, nível no SOC e artefato por etapa correspondem, respectivamente, aos requisitos R1, R3 e R2. Trata-se de comparação qualitativa, feita pelos próprios autores, limitação registrada no Quadro 15.

Quadro 12. Estudos próximos: objeto, base normativa e lacuna em relação a este artigo

Estudo	Objeto	Base normativa	Lacuna em relação a este artigo

Biskup e Flegel (2000)	Pseudônimos em dados de auditoria para detecção de intrusão.	Anterior ao RGPD e à LGPD.	Hipóteses legais, regulação setorial e artefatos de governança.
Menges *et al.* (2021)	Requisitos do RGPD para SIEM e arquitetura com pseudonimização, com análise do efeito sobre a detecção.	RGPD.	LGPD, regulação setorial brasileira e CLT.
Robles-González, Parra-Arnau e Forné (2020)	LINDDUN aplicado a identificação e autenticação.	Sem ancoragem na LGPD.	Demais elementos do *pipeline* e hipóteses legais.
Hernandez-Ramos *et al.* (2025)	Revisão sistemática da detecção de intrusão por aprendizado federado.	Sem ancoragem na LGPD.	Governança jurídica do tratamento e dimensão laboral.
Brasil (2023b)	Modelo de política de registros de auditoria para órgãos federais.	Normas federais de segurança da informação.	Setor privado, hipóteses legais por cenário e matriz de ameaças.
Cardoso e Gualberto (2026)	Princípios do art. 6º da LGPD convertidos em controles para *logs* de autenticação, validados em SIEM.	LGPD (art. 6º).	EDR, DLP e UEBA, hipóteses legais por cenário e relação de emprego.
Resende, Portes Filho e Santos Filho (2026)	Anonimização automatizada em *pipelines* de ETL, com *k*-anonimato.	LGPD.	Telemetria de segurança e reidentificação controlada.

Este artigo	*Pipeline* do SOC da coleta à reidentificação, com artefato por passo.	LGPD, CF, CLT e regulação do CMN e do BCB.	Validação empírica e por especialistas (Seção 6.3).

Fonte: Elaborado pelos autores (2026), com base nas fontes citadas. ETL = extração, transformação e carga.

Quadro 13. Comparação entre o *framework* proposto e referenciais existentes

Referencial	Unidade de análise	Ancoragem na LGPD	Nível no SOC	Artefato por etapa
Privacy by Design (Cavoukian, 2009)	Princípios organizacionais	Indireta (art. 46, § 2º)	Baixo	Não
STRIDE (Shostack, 2014)	Ameaças à segurança	Nenhuma	Alto	Modelo de ameaças
LINDDUN (Deng *et al.*, 2011; Sion *et al.*, 2025)	Ameaças à privacidade	Nenhuma	Alto	Modelo de ameaças
NIST *Privacy Framework* (NIST, 2020)	Riscos de privacidade da organização	Nenhuma	Médio	Perfis de implementação
ISO/IEC 27701 (ABNT, 2019; ISO, 2025)	Gestão da privacidade	Indireta (anexo de correspondência na edição ABNT de 2019; edição ISO	Médio	Controles certificáveis

		autônoma de 2025)		
Guia de legítimo interesse (ANPD, 2024a)	Uma hipótese legal	Direta (arts. 7°, IX, e 10)	Baixo	Teste de balanceamento
ICO (2023) e CNIL (2021)	Monitoramento laboral e *logs*	Nenhuma	Médio	Recomendações e prazos
Cardoso e Gualberto (2026)	*Logs* de autenticação	Direta (art. 6°)	Médio	Controles por princípio
Modelo de política de *logs* (Brasil, 2023b)	Registros de auditoria federais	Indireta	Médio	Modelo de política
Framework proposto	*Pipeline* de dados do SOC	Direta, por dispositivo	Alto	Sim (Quadro 3 e Apêndice B)

Fonte: Elaborado pelos autores (2026), sobre as versões citadas. A ancoragem é direta quando o referencial cita dispositivos da LGPD, indireta quando a alcança por anexo ou princípio e nenhuma quando não se refere à LGPD. O nível no SOC é baixo para princípios sem objeto técnico, médio para controles ou recomendações sobre registros e alto para ameaças ou decisões por elemento do *pipeline*. Os estudos acadêmicos próximos estão no Quadro 12.

Quadro 14. Correspondência indicativa entre os passos do *framework* e controles ou categorias de referenciais de mercado

Passo	ISO/IEC 27002 (controles)	ISO/IEC 27701 (cláusulas)	NIST CSF 2.0	NIST *Privacy Framework*
1 Finalidade	5.9 e 8.16	7.2.1 e 7.2.8	ID.AM-07 e DE.CM	ID.IM-P
2 Base legal	5.31 e 5.34	7.2.2 e 7.2.5	GV.OC-03	ID.RA-P e GV.PO-P
3 Necessidade e minimização	5.33 e 8.10	7.4.1, 7.4.4 e 7.4.7	ID.AM-08	CT.DM-P
4 Salvaguardas técnicas	5.15, 8.2, 8.11 e 8.24	7.4.5	PR.AA e PR.DS	CT.DP-P, PR.AC-P e PR.DS-P
5 Transparência ativa	5.34	7.3.2, 7.3.3 e 7.3.10	Sem correspondente	CM.AW-P
6 Auditabilidade	5.35 e 8.15	7.2.8	GV.OV e ID.IM	GV.MT-P

Fonte: Elaborado pelos autores (2026), com base em ABNT (2019, 2022b) e NIST (2020, 2024). O artefato de cada passo pode servir de evidência para o controle ou a categoria indicados. A numeração da 27701 segue a edição da ABNT de 2019.

Quadro 15. Avaliação *ex ante* dos requisitos do *framework*: critério, evidência, resultado e limitação

Requisito	Critério observável	Evidência no artefato	Resultado	Limitação

R1 Ancoragem normativa	Cada passo indica dispositivos da LGPD.	Quadros 1, 3 e 9.	Atendido	Leituras dos arts. 7º, VI, e 11, II, *g*, adotadas como tese interpretativa, com exposição da tese contrária (Seção 2.3). O art. 13, § 4º, é aplicado fora dos estudos em saúde, e não houve validação por especialistas.
R2 Artefato verificável por passo	Cada passo gera documento auditável por terceiro.	Quadros 3 e 7 a 11, Figura 2 e Passos 1 a 6 instanciados na Seção 5.4.	Atendido no desenho	Modelos não testados em organização real (Seção 6.3).
R3 Aplicabilidade ao SOC	Cada passo atua sobre ao menos um elemento do *pipeline*.	Figura 1 e Quadros 2, 4, 9 e 17.	Atendido no desenho	Demonstração restrita a um evento de UEBA e a um cenário de pequeno porte (Seção 6.3).
R4 Explicitação de *trade-offs*	Tensões e conflitos nomeados, com controle de conciliação ou decisão de escopo.	Quadros 2 e 18, além da Seção 6.1.	Atendido no desenho	Critério de retenção por percentil (Seção 6.1) proposto como hipótese operacional, sem calibração e dependente de

				distribuições setoriais raramente publicadas.
R5 Proporcionalidade ao porte	Perfil reduzido para pequeno porte.	Apêndice D e Seção 5.2 (serviço gerenciado de chaves).	Em parte	Perfil preliminar, sem estimativa quantitativa de custos.
R6 Compatibilidade com referenciais	Comparação explícita com estudos e referenciais existentes.	Quadros 12, 13 e 14.	Atendido	Comparação qualitativa, feita pelos autores.

Fonte: Elaborado pelos autores (2026). Procedimento descrito na Seção 3.2, que combina argumentação fundamentada e demonstração em cenário (Venable; Pries-Heje; Baskerville, 2016), nos níveis de consistência interna e demonstração. Os limites estão na Seção 6.3.

Quadro 16. Índice de priorização: práticas de monitoramento, propensão, impacto e relevância regulatória

Prática analisada	Dispositivos normativos	P	I	Nível	Relevância regulatória
Retenção ilimitada de *logs* de SIEM, sem expurgo.	Art. 6º, III e VII, e arts. 15 e 16.	3	2	Alto	Média

⚠ Esta tabela possui muitas colunas e foi cortada para impressão. Para visualizá-la completa, acesse o artigo original em: https://revistatopicos.com.br/artigos/framework-de-governanca-para-o-monitoramento-proporcional-em-centros-de-operacoes-de-seguranca-sob-a-lgpd?noblockage

Fonte: Elaborado pelos autores (2026), com base na ISO/IEC 27005 (ISO, 2022) e no art. 8º do regulamento de dosimetria (ANPD, 2023a). P indica propensão e I, impacto. As notas resultam de julgamento fundamentado, e o nível segue a matriz da Seção 4.2. A relevância "média ou grave" passa a ser grave se ocorrer circunstância do art. 8º, § 3º, do regulamento, como dados sensíveis de familiares (EDR) ou tratamento sem hipótese legal ou discriminatório (reuso).

Nenhuma prática é crítica. As de impacto 3 pressupõem decisão de política, e a única com P = 3 tem impacto 2. Na análise de sensibilidade, variar uma nota em um ponto altera o nível de todas as práticas, exceto a linha de base. Se a propensão das três práticas de P 2 × I 3 cair para 1, elas descem ao nível médio (3) e ficam abaixo do UEBA (4), que, com P = 3, sobe para 6 e empata com o grupo alto.

APÊNDICE D - SEGUNDO CENÁRIO: AGENTE DE PEQUENO PORTE NÃO REGULADO

Para agentes de pequeno porte, que em regra podem dispensar o encarregado, mas devem manter canal de comunicação com o titular (ANPD, 2022, art. 11), o artigo propõe um perfil preliminar, que inclui registro simplificado da hipótese legal, prazos de expurgo nativos ou contratados, vedação de captura de conteúdo, aviso interno, cláusulas de operador (art. 39) e chaves em serviço gerenciado sob controle do controlador. O segundo cenário retrata uma desenvolvedora de *software* hipotética, agente de tratamento

de pequeno porte, com 40 colaboradores em teletrabalho que usam dispositivos pessoais, sem obrigação setorial de segurança e sem encarregado indicado. A finalidade é detectar *malware* e acesso indevido ao código-fonte e a dados de clientes.

As dispensas do pequeno porte deixam de valer quando o tratamento é de alto risco (ANPD, 2022, art. 3º). Pelo art. 4º do regulamento, o alto risco exige ao menos um critério geral e um específico. Entre os gerais, a larga escala está afastada pelo número de titulares, mas o monitoramento de trabalhadores pode afetar significativamente seus interesses e direitos fundamentais. Entre os específicos, incidiria a decisão unicamente automatizada se o EDR isolasse dispositivos ou bloqueasse contas sem revisão humana. Incidiriam também o critério de uso de dados sensíveis, se o escopo vazasse para a vida privada, e o de uso de tecnologia emergente, conforme a avaliação do controlador sobre os modelos do EDR. O escopo restrito ao contêiner reduz o risco de vazamento para a vida privada, mas não define, isoladamente, o enquadramento, que depende do conjunto das circunstâncias e deve ser registrado no Passo 2. Quando há alto risco, o perfil reduzido deixa de se aplicar e o RIPD passa a ser recomendado. O Quadro 17 aplica os seis passos sob a premissa de respostas automáticas sujeitas a revisão humana.

Quadro 17. Passos do *framework* no cenário de pequena empresa não regulada

Passo	Decisão no cenário	Artefato simplificado
1 Finalidade	Detectar *malware* e acesso indevido a repositórios de código e a dados de clientes, sem incluir a produtividade.	Lista de casos de uso com fonte e regra.

2 Base legal	Legítimo interesse (arts. 7º, IX, e 10), sem obrigação setorial e com análise dos critérios de alto risco. O consentimento é descartado pela assimetria do emprego.	Teste de balanceamento simplificado, análise de alto risco (ANPD, 2022, art. 4º) e registro simplificado das operações.
3 Necessidade e minimização	EDR restrito aos processos e conexões do contêiner corporativo, sem navegação pessoal, arquivos pessoais ou geolocalização, e retenção ilustrativa de seis meses.	Dicionário de dados e prazos configurados no fornecedor.
4 Salvaguardas técnicas	Serviço de EDR em nuvem com chaves sob controle da empresa em serviço gerenciado, acesso restrito a dois administradores, autenticação multifator, cláusulas de operador (art. 39) e respostas automáticas sujeitas a revisão humana.	Contrato com o operador e lista de acessos.
5 Transparência ativa	Escopo no contrato escrito de teletrabalho (arts. 75-C e 75-D da CLT) e aviso interno. O contrato não substitui o teste de balanceamento.	Aviso e canal de comunicação com o titular (ANPD, 2022, art. 11).
6 Auditabilidade	Registro das consultas dos administradores e revisão semestral pelo responsável pelo canal, que assume as consultas atribuídas ao encarregado.	Relatório semestral simplificado.

Fonte: Elaborado pelos autores (2026). Cenário hipotético, com números e prazos ilustrativos. Sem obrigação setorial, toda a base recai no legítimo interesse, tornando decisivo o Passo 2.

APÊNDICE E - RELAÇÕES ENTRE AMEAÇAS STRIDE E LINDDUN NO *PIPELINE* DO SOC

Quadro 18. Matriz STRIDE + LINDDUN detalhada: ativo, ameaça, dado pessoal, efeito, conciliação e risco residual (pares representativos)

Elemento e ativo	Ameaça STRIDE e controle de segurança	Dado pessoal e efeito LINDDUN	Relação	Conciliação	Risco residu
Fonte (estações e contas)	*Spoofing* (credencial roubada), combatido por autenticaç	Identificador da conta, sujeito a *Linking* entre	Tensão	Pseudônimo determinístico, com correspondência em	*Linking* entre sessões permar e, reduz pela

⚠ Esta tabela possui muitas colunas e foi cortada para impressão. Para visualizá-la completa, acesse o artigo original em: https://revistatopicos.com.br/artigos/framework-de-governanca-para-o-monitoramento-proporcional-em-centros-de-operacoes-de-seguranca-sob-a-lgpd?noblockage

Fonte: Elaborado pelos autores (2026), com base em Shostack (2014), Deng *et al.* (2011), Robles-González, Parra-Arnau e Forné (2020) e Sion *et al.* (2025). Cada linha é um par representativo de uma matriz muitos-para-muitos.

Quatro associações da matriz exigem esclarecimento específico quanto ao enquadramento adotado. Na primeira, a detecção de *Spoofing* requer a vinculação de eventos à mesma conta. O controle é a autenticação, e a correlação exige identificador estável, razão pela qual a tensão recai sobre *Linking* e *Identifying* (Robles-

González; Parra-Arnau; Forné, 2020). A telemetria de fluxo por dispositivo, necessária para localizar a estação usada em ataque volumétrico, revela horários e hábitos e configura *Detecting* e *Linking*. A preservação do sinal com agregação por sub-rede é hipótese a testar na prova de conceito. A imutabilidade contra adulteração impede o expurgo e a eliminação a pedido, mas a expiração por partição concilia essas exigências.

A quarta associação, a do não repúdio, foi classificada como conflito. Para a mesma ação privada, nenhum dos controles examinados assegura simultaneamente a atribuição exigida pela segurança e a negabilidade valorizada pela privacidade (Deng *et al.*, 2011). Diante do conflito, a regra de decisão do livro de códigos determina a delimitação do escopo. Nos coletores, essa decisão traduz-se na política de coleta dos agentes de EDR e nas regras de ingestão do SIEM. Recebem registro nominal, com não repúdio apoiado na trilha de auditoria, apenas os processos executados com privilégio elevado (como *token* elevado ou nível de integridade alto ou de sistema no Windows e execução via *sudo* no Linux) e as sessões de contas administrativas retiradas de cofre de gestão de acesso privilegiado (PAM). A escolha segue os controles de direitos de acesso privilegiado e de registro de eventos (ABNT, 2022b, controles 8.2 e 8.15). Os eventos das contas comuns seguem sob pseudônimo e, em dispositivo pessoal, a coleta limita-se ao contêiner corporativo, de modo que as ações privadas não recebem registro nominal. O DLP sobre os repositórios não é proposto como controle complementar da exfiltração, pois acrescentaria vigilância sobre os analistas sem reduzir a ameaça à privacidade do par.

[1] Discente do Curso de Bacharel em Engenharia de Software da Universidade de Vassouras, *Campus* Maricá. Av. Roberto Silveira, 1954, Flamengo, Maricá, RJ, CEP 24903-815. ORCID: https://orcid.org/0009-0004-9146-2012. E-mail: acesse o artigo original para visualizar o e-mail

[2] Discente do Curso de Bacharel em Engenharia de Software da Universidade de Vassouras, *Campus* Maricá. Av. Roberto Silveira, 1954, Flamengo, Maricá, RJ, CEP 24903-815. ORCID: https://orcid.org/0009-0004-2650-8571. E-mail: acesse o artigo original para visualizar o e-mail

[3] Discente do Curso de Bacharel em Engenharia de Software da Universidade de Vassouras, *Campus* Maricá. Av. Roberto Silveira, 1954, Flamengo, Maricá, RJ, CEP 24903-815. ORCID: https://orcid.org/0009-0007-8356-6948. E-mail: acesse o artigo original para visualizar o e-mail

[4] Discente do Curso de Bacharel em Engenharia de Software da Universidade de Vassouras, *Campus* Maricá. Av. Roberto Silveira, 1954, Flamengo, Maricá, RJ, CEP 24903-815. ORCID: https://orcid.org/0009-0007-8473-3955. E-mail: acesse o artigo original para visualizar o e-mail

[5] Doutora em Bioquímica pela Universidade Federal do Rio de Janeiro. Docente do Curso de Bacharel em Engenharia de Software da Universidade de Vassouras, *Campus* Maricá. Av. Roberto Silveira, 1954, Flamengo, Maricá, RJ, CEP 24903-815. ORCID: https://orcid.org/0000-0003-3825-7242. E-mail: acesse o artigo original para visualizar o e-mail

[6] Mestre em Gestão do Trabalho pela Universidade Santa Úrsula. Docente do Curso de Bacharel em Engenharia de Software da Universidade de Vassouras, *Campus* Maricá. Av. Roberto Silveira, 1954, Flamengo, Maricá, RJ, CEP 24903-815. ORCID: https://orcid.org/0000-0002-9377-5993. E-mail: acesse o artigo original para visualizar o e-mail

[7] A Autoridade Nacional de Proteção de Dados foi transformada em Agência Nacional de Proteção de Dados pela Lei nº 15.352, de 25 de fevereiro de 2026, conversão da Medida Provisória nº 1.317/2025, que deu nova redação ao art. 55-A da LGPD (Brasil, 2026). A sigla foi mantida e, nas referências, todos os atos foram reunidos sob a denominação original, para padronizar a entrada.

[8] O regulamento europeu classifica como de alto risco os sistemas de IA que monitoram trabalhadores (anexo III, ponto 4, *b*), com obrigações adiadas para dezembro de 2027.