Privacidade em Logs de Autenticação nas IFES: Um Guia técnico de conformidade com a LGPD

Gelson Barros Cardoso
Gelson.cardoso@gestao.gov.br
Universidade de Brasília (UNB)
Brasil

Éder Souza Gualberto
eder.gualberto@redes.unb.br
Universidade de Brasília (UNB)
Brasil

Resumo

Os registros de logs de autenticação constituem um ativo essencial para a cibersegurança, auditoria, resposta a incidentes e investigações forenses nas Instituições Federais de Ensino Superior (IFES). Contudo, tais registros frequentemente contêm dados que permitem a identificação direta ou indireta de indivíduos, submetendo-os às exigências da Lei Geral de Proteção de Dados Pessoais (LGPD). Embora a privacidade de dados seja um tema amplamente estudado em diferentes contextos e domínios, o registro de autenticação nas IFES ainda permanece pouco explorado. Diante desse cenário, este artigo tem como objetivo propor um guia técnico voltado à gestão de logs de autenticação para IFES em conformidade com a LGPD. Para tanto, realizou-se uma revisão bibliográfica e análise documental da legislação vigente, bem como de normas e boas práticas de segurança da informação amplamente adotadas. Como resultado, apresenta-se um guia técnico que operacionaliza os princípios da LGPD por meio de recomendações voltadas à gestão de logs de autenticação em ambientes de IFES.

Palavras-chave: Logs de autenticação, Privacidade, LGPD, Segurança da informação, Conformidade.

Introdução

Em um panorama digital marcado por crescentes volumes de dados e sofisticação de ameaças cibernéticas, os registros de eventos (logs) consolidaram-se como um componente essencial das estratégias de segurança da informação. Esses registros desempenham papel central na detecção de incidentes, na resposta a ataques, na análise forense, na auditoria de conformidade e no monitoramento da integridade e disponibilidade dos sistemas (CHUVAKIN; SCHMIDT; PHILLIPS, 2012; KENT; SOUPPAYA, 2006).

Os logs de autenticação constituem um dos principais mecanismos de identificação do usuário ou entidade no contexto da segurança da informação, registrando eventos relacionados ao acesso a sistemas, redes, aplicações e infraestruturas de Tecnologia da Informação (TI). Esses registros normalmente incluem informações como identificador do usuário, data e hora de acesso, endereço IP de origem, resultado da tentativa de autenticação e outros metadados (ABNT 27002, 2022; KENT; SOUPPAYA, 2006). No entanto, à medida que se tornam mais detalhados e abrangentes, os registros

de autenticação passam a incluir dados pessoais e até Dados Pessoais Sensíveis (DPS), ampliando os riscos relacionados à privacidade.

Essa realidade impõe desafios significativos no contexto da LGPD, uma vez que eventos registrados em logs de autenticação não são apenas registros técnicos, mas a memória operacional das atividades de acesso em uma organização, que pode conter informações capazes de permitir a identificação de indivíduos (CHUVAKIN; SCHMIDT; PHILLIPS, 2012; VILELA, 2017). Sob essa ótica, proteger a privacidade é fundamental não apenas para atender às exigências regulatórias, mas também para manter a confiança dos usuários e evitar potenciais danos decorrentes de vazamentos de dados.

Apesar de documentos normativos e frameworks nacionais tratarem da governança e da gestão de logs no setor público (GSI/PR, 2014b; BRASIL, 2025), suas diretrizes concentram-se predominantemente em requisitos voltados à resiliência operacional, ao monitoramento e à resposta a incidentes cibernéticos. Observa-se, entretanto, uma lacuna quanto à convergência entre privacidade e segurança da informação, pois estudos demonstram que equipes técnicas frequentemente enfrentam dificuldades para interpretar requisitos abstratos de privacidade e traduzi-los em arquiteturas e mecanismos de proteção efetivamente implementáveis (PEIXOTO et al., 2023; CANEDO et al., 2022; ROCHA, et al., 2023; CANEDO et al., 2025).

O desafio torna-se ainda mais significativo nas Instituições Federais de Ensino Superior (IFES), caracterizadas por ecossistemas de identidade digitais heterogêneos, distribuídos e administrados por múltiplas unidades organizacionais. Nesse contexto, surge a problemática desta pesquisa: como as IFES podem conciliar a necessidade de coleta de dados em logs de autenticação com as restrições impostas pela LGPD? Diante desse cenário, o objetivo deste artigo é propor um guia técnico para a gestão de logs de autenticação em IFES alinhado à LGPD, operacionalizando os princípios da lei por meio de mecanismos práticos de engenharia de privacidade.

2. Fundamentação Teórica

2.1. Registros de Logs na Segurança da Informação

Segundo Chuvakin, Schmidt e Phillips (2012), os registros de logs constituem a memória operacional e de segurança de sistemas de informação, funcionando como uma camada fundamental de visibilidade sobre as atividades que ocorrem em redes, servidores, aplicações e dispositivos de segurança. Mais do que meros arquivos de registro, os logs permitem estabelecer uma linha do tempo auditável de ações, sendo essenciais para a detecção de incidentes, a investigação forense, a responsabilização de usuários e a verificação da integridade operacional dos sistemas (CHUVAKIN; SCHMIDT; PHILLIPS, 2012).

De acordo com Araujo et al. (2024), além da segurança, os logs desempenham um papel vital na observabilidade operacional das infraestruturas de TI. Eles fornecem visibilidade sobre o desempenho de aplicações, gargalos de rede e comportamentos anômalos que, embora nem sempre representem ataques deliberados, podem indicar

falhas de configuração ou degradação de hardware. Portanto, a gestão estratégica desses dados permite uma transição do monitoramento passivo para uma postura de observabilidade proativa, onde os dados de log servem como base para a tomada de decisão executiva e conformidade regulatória (ARAUJO et al., 2024).

Nessa perspectiva, o papel dos logs extrapola a função técnica de simples registro de eventos, consolidando-se como um ativo estratégico para a governança de tecnologia da informação (TI) e para o fortalecimento da postura de segurança organizacional. Logo, quando gerenciados de forma estruturada, esses registros viabilizam não apenas a rastreabilidade e a investigação de incidentes, mas também o suporte a auditorias, à conformidade regulatória e à tomada de decisão baseada em evidências.

De acordo com o Guia do Framework de Privacidade e Segurança da Informação (PPSI 2.0) (BRASIL, 2025), existem duas categorias principais de logs que são comumente gerenciadas de maneira distinta, os logs de sistema e os logs de auditoria. Enquanto os primeiros são nativos e registram eventos operacionais, como inicializações e falhas de processos, exigindo configuração mínima para ativação, os logs de auditoria concentram-se em ações dos usuários como acessos a recursos, execução de operações sensíveis e tentativas de autenticação. Nesse contexto, os logs de autenticação são usualmente classificados como um subtipo de logs de auditoria, uma vez que documentam eventos diretamente relacionados ao processo de verificação de identidade e controle de acesso aos sistemas.

2.2. Registro de Auditoria em Logs de Autenticação

Logs de autenticação são registros especializados no monitoramento de acessos e na verificação de identidades em sistemas de informação. Fundamentais para a governança de TI, eles funcionam como uma trilha detalhada que documenta desde tentativas de login até o uso efetivo de redes e recursos da organização. Esses registros são gerados por sistemas operacionais, aplicações, serviços de rede e plataformas de gerenciamento de identidade, registrando interações relacionadas ao processo de autenticação de usuários.

De acordo com as diretrizes da Associação Brasileira de Normas Técnicas -ABNT 27002 (2022) e do Guia do PPSI 2.0 (BRASIL, 2025), a eficácia do monitoramento depende da captura detalhada de eventos em nível de usuário, abrangendo não apenas registros de data e hora de autenticação, mas também o rastreamento rigoroso de acessos permitidos e bloqueados pelo sistema. Além disso, a norma ABNT 27002 (2022) também recomenda uma lista de doze procedimentos para o registro de entrada em um sistema ou aplicativo para minimizar o risco de acesso não autorizado, conforme a tabela a seguir.

Tabela 1 – Procedimento seguro para entrada no sistema.

Item	Detalhamento
a	não exibir informações sensíveis do sistema ou do aplicativo até que o processo de log-on no sistema tenha sido concluído com sucesso, a fim de evitar fornecer a um usuário não autorizado

	qualquer assistência desnecessária;
b	exibir um aviso público de que convém que o sistema, aplicativo ou serviço só sejam acessados por usuários autorizados;
c	não fornecer mensagens de ajuda durante o procedimento de acesso ao sistema que auxiliariam um usuário não autorizado (por exemplo, se houver uma condição de erro, não convém que o sistema indique qual parte dos dados está correta ou incorreta);
d	validar as informações de log-on no sistema somente na conclusão de todos os dados de entrada;
e	proteger contra tentativas de log-on com força bruta em nomes de usuário e senhas (por exemplo, usando o CAPTCHA, exigindo redefinição de senha após um número predefinido de tentativas fracassadas ou bloqueando o usuário após um número máximo de erros);
f	registrar as tentativas malsucedidas e bem-sucedidas;
g	criar um evento de segurança, se for detectada uma possível tentativa ou violação bem-sucedida de controles de acesso ao sistema (por exemplo, enviando um alerta para o usuário e os administradores do sistema da organização quando um determinado número de tentativas erradas de senha foi alcançado);
h	exibir ou enviar as seguintes informações em um canal separado na conclusão de um acesso bem-sucedido: 1) data e hora do log-on anterior bem-sucedido ao sistema; 2) detalhes de quaisquer tentativas de log-on malsucedidas desde o último log-on bem-sucedido ao sistema;
i	não exibir a senha em texto puro quando ela estiver sendo inserida; em alguns casos, pode ser necessário desativar essa funcionalidade para facilitar o acesso ao sistema pelo usuário (por exemplo, por razões de acessibilidade ou para evitar o bloqueio de usuários por causa de erros repetidos);
j	não transmitir senhas em texto puro pela rede para evitar a captura por um programa de “sniffer” de rede;
k	finalizar sessões inativas após um período especificado de inatividade, especialmente em locais de alto risco, como áreas públicas ou externas fora da gestão de segurança da organização ou em dispositivos de terminal do usuário;
l	restringir os tempos de duração da conexão para fornecer segurança adicional para aplicações de alto risco e reduzir a janela de oportunidade para acesso não autorizado.

Fonte: ABNT ISO/IEC 27002 (2022)

Conforme se verifica na Tabela 1, o registro sistemático de tentativas de acesso (itens f, g, h) constitui um dos pilares do procedimento seguro de entrada. Contudo, a norma vai além das práticas de entrada no sistema, pois para que esse registro cumpra sua função de auditoria e responsabilização, a própria ABNT 27002 (2022) define um conjunto mínimo de informações que devem ser capturadas em cada evento de log de autenticação, apresentado na Tabela 2.

Tabela 2 – O que deve ser registrado

O que deve ser registrado	Exemplos práticos
Identificador único do usuário que executou a ação	login joao.silva, ID do usuário, conta de serviço
Timestamp preciso do evento	2025-08-08 16:20:45 UTC
Se a operação foi bem-sucedida ou falhou	sucesso, falha, bloqueado
Origem da conexão ou ação	IP de origem, hostname, dispositivo
Sistema ou aplicação que gerou o evento	servidor LDAP, aplicação web, firewall
Identificador da sessão ou transação	session ID em aplicação web
Combinação de múltiplos fatores	o que você sabe, o que você tem e o que você é

Fonte: Adaptado da ABNT (2022)

Conforme demonstrado na Tabela 2, os registros de autenticação permitem acompanhar quando, como e a partir de onde um usuário tenta acessar determinado recurso computacional. De acordo com a ABNT (2022), referente à autenticação segura, os principais eventos do registro de logs de autenticação são: o login bem-sucedido, que indica a validação correta das credenciais de acesso; as falhas de autenticação, que registram tentativas inválidas de login; o logout, que documenta o encerramento da sessão pelo usuário ou pelo sistema; o bloqueio de conta, geralmente acionado após múltiplas tentativas de acesso malsucedidas; e a autenticação multifator (MFA), que registra a utilização de fatores adicionais de verificação de identidade.

Em relação aos atributos essenciais dos logs, tanto a norma ABNT NBR 27001 (2024) quanto o guia NIST SP 800-92 (Kent & Souppaya, 2006) recomendam a coleta de dados que permitam o rastreamento das atividades. Isso inclui registrar a identificação do usuário (ID do usuário/username), o endereço IP de origem da conexão, o timestamp do evento e informações sobre o serviço que foi acessado.

2.3. A LGPD no Contexto Técnico de Logs de Autenticação

A publicação da Lei Geral de Proteção de Dados Pessoais (LGPD) em 2018 instituiu um marco regulatório significativo para o tratamento de dados pessoais no Brasil, impactando diretamente as práticas de gestão de informações em ambientes organizacionais. A legislação estabelece que o tratamento de qualquer dado pessoal, incluindo os dados contidos em registros de logs de autenticação, deve observar estritamente os princípios da LGPD. Além disso, o descumprimento dessas disposições sujeita o controlador a penalidades, aplicadas pela Agência Nacional de Proteção de Dados (ANPD), incluindo advertências, multas e bloqueio dos dados.

No contexto específico dos logs de autenticação, a LGPD (BRASIL, 2018) determina que toda informação capaz de identificar, direta ou indiretamente, um

indivíduo, como matrícula, CPF, endereços IP, dados biométricos e informações de dispositivo, configura dados pessoais ou DPS. Dessa forma, o processamento desses registros deve observar os princípios e as bases legais previstos na lei, o que implica a aplicação de requisitos técnicos de proteção de dados, para além de sua função operacional.

Entre os princípios estabelecidos pela LGPD, destaca-se o da transparência, que assegura ao titular o direito de compreender como seus dados são coletados, utilizados e armazenados, mantendo, assim, o controle sobre sua identidade digital em um ambiente cada vez mais orientado por dados. Para garantir essa proteção, o Art. 6º da lei define dez princípios fundamentais que orientam o tratamento de dados pessoais em qualquer contexto, seja por pessoas físicas ou jurídicas, de direito público ou privado. A Tabela 3 apresenta, de forma sintética, esses princípios e seus respectivos desdobramentos.

Tabela 3 – Princípios da LGPD

Princípios	Detalhamento
Finalidade	O tratamento deve ser feito para propósitos legítimos, específicos e informados ao titular, sem possibilidade de uso posterior incompatível.
Adequação	Os dados tratados devem ser compatíveis com a finalidade que foi informada ao usuário.
Necessidade	A coleta deve ser limitada ao mínimo necessário para atingir a finalidade, evitando o excesso de dados.
Livre Acesso	Garantia de consulta facilitada e gratuita aos titulares sobre a forma, duração e integralidade de seus dados.
Qualidade dos Dados	Garantia de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade do tratamento.
Transparência	Informações claras, precisas e acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento.
Segurança	Utilização de medidas técnicas e administrativas para proteger os dados de acessos não autorizados e situações acidentais.
Prevenção	Adoção de medidas para evitar a ocorrência de danos em virtude do tratamento de dados pessoais.
Não Discriminação	Impossibilidade de realizar o tratamento para fins discriminatórios, ilícitos ou abusivos.
Responsabilização	Demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento da lei.

Fonte: Adaptado de Brasil (2018)

A utilização desses princípios ao contexto técnico dos logs de autenticação impõe desafios práticos às equipes de infraestrutura e segurança da informação. Tal cenário ocorre porque os dados frequentemente registrados, como endereços IP, identificadores

de usuário e informações de dispositivo, podem, isoladamente ou em conjunto, permitir a inferência de comportamentos, padrões de acesso e até mesmo localização dos titulares dos dados (KUNIMOTO; OKUBO, 2023).

2.4 Normas Técnicas e Frameworks Aplicáveis à Gestão de Logs

A convergência entre segurança e privacidade é operacionalizada por meio da adoção de padrões internacionais, como a família ABNT ISO/IEC 27000. Enquanto a ABNT 27001 e 27002 estabelecem os controles de segurança e gestão de logs de auditoria, a ABNT 27701 (2020) estende esses requisitos para a gestão da privacidade, criando um Sistema de Gestão de Informação de Privacidade (PIMS). Complementarmente, o NIST SP 800-92 oferece diretrizes granulares sobre a infraestrutura de gerenciamento de logs, detalhando desde a geração até a análise, o que permite que profissionais de TI estruturem sistemas resilientes e auditáveis.

O NIST SP 800-92 estabelece que o gerenciamento de logs deve ser planejado em conjunto com a área de privacidade para assegurar a proteção dos dados. Além disso, o documento também recomenda evitar a gravação de informações sensíveis desnecessárias, como senhas, limitando a coleta ao estritamente exigido para reduzir riscos de acessos não autorizados. Por fim, recomenda que as políticas organizacionais devem determinar procedimentos claros para tratar conteúdos confidenciais que venham a ser registrados acidentalmente.

De acordo com ABNT 27002 (2022), o controle 8.15 estabelece que os logs devem registrar eventos como tentativas de acesso a sistemas e dados, alterações de configuração, uso de privilégios elevados e atividades de administração de identidades, exigindo que cada registro contenha metadados mínimos como identificador de usuário, data/hora, tipo de evento e identificadores de dispositivo. Essa abrangência, contudo, impõe desafios significativos: a geração de logs em volume massivo, se não planejada, pode resultar em custos elevados de armazenamento e processamento, além de dificultar a análise efetiva por meio de ferramentas automatizadas como sistemas SIEM (Security Information and Event Management).

A ABNT 27002 (2022) também recomenda que as organizações implementem procedimentos automatizados para excluir ou desidentificar logs em conformidade com políticas de retenção publicadas, priorizando o monitoramento contínuo e automatizado de acessos a informações pessoais. Portanto, a ausência desses controles técnicos não apenas expõe a organização a riscos de violação de dados, mas também compromete sua capacidade de demonstrar conformidade perante auditorias e fiscalizações.

A norma ABNT 27701(2020) preconiza a necessidade de um processo contínuo, periódico e documentado de análise crítica dos registros de eventos. O documento também orienta que, sempre que viável, os dados pessoais sejam armazenados para garantir a rastreabilidade, identificando a autoria do acesso, o momento da ocorrência e as modificações realizadas. De forma complementar, o Anexo A da norma ABNT 27557 (2023) fornece uma tabela com exemplos práticos destinados a auxiliar na identificação e no mapeamento das diferentes categorias de dados pessoais:

> "Estado civil, identidade, dados de identificação (número de identificação) Dados de contato (telefone, endereço, email etc.) Vida pessoal (hábitos, estado civil, posições filosóficas, políticas, religiosas e sindicais, vida sexual, dados de saúde, origem racial ou étnica, crimes/condenações etc. – excluindo dados sensíveis ou perigosos) Vida profissional (currículo, educação e treinamentos profissionais, prêmios etc.) Informação econômica e financeira (dados bancários, rendimentos, situação financeira, situação fiscal etc.) Dados de conexão (endereços IP, logs de eventos etc.) Dados de localização (viagens, dados de GPS, dados de GSM etc.) Credenciais (PIN, senhas, dados de autenticação baseados em conhecimento etc.) Dados biométricos"

No âmbito nacional, o Guia do Framework de Privacidade e Segurança da Informação (PPSI) (BRASIL, 2025) surge como um referencial essencial para a administração pública no Brasil, incluindo as exigências da LGPD em controles e medidas. Ao integrar recomendações da OWASP e do CIS Controls, o Guia PPSI 2.0 fornece uma camada de maturidade que auxilia na implementação de registros de eventos que não apenas detectam falhas, mas que também respeitam o ciclo de vida do dado. A seguir, a Tabela 4 apresenta um resumo dos principais frameworks internacionais e nacionais relevantes.

Tabela 4 – Principais Normas e Framework

Framework/ Norma	Detalhamento
ABNT NBR 27001	Estabelece requisitos gerais para um Sistema de Gestão de Segurança da Informação (SGSI), incluindo controles de registro de eventos como parte do Anexo A, visando assegurar a disponibilidade, integridade e confidencialidade dos logs para suporte a auditorias e resposta a incidentes.
ABNT NBR 27002	Oferece um guia de boas práticas para implementação dos controles da ISO 27001, detalhando como planejar, proteger, reter e revisar logs, com ênfase na integridade e confidencialidade das informações registradas.
ABNT NBR 27701	Extensão da ISO 27001 para privacidade, focando no tratamento de dados pessoais; requer que os logs capturem acessos, consentimentos e operações sobre dados pessoais, assegurando a rastreabilidade e a proteção desses registros.
NIST SP 800-92	Publicação técnica dedicada exclusivamente à gestão de logs, abordando todo o ciclo de vida: planejamento, coleta, armazenamento, análise e descarte, com foco em segurança, integridade e utilidade para detecção de incidentes.
OWASP	Guia de boas práticas para segurança em aplicações web; recomenda logging específico de eventos de segurança, alertando para não inclusão de dados sensíveis e propondo formatos estruturados para facilitar a análise automatizada.
CIS Controls	Conjunto de ações prioritárias para defesa cibernética; o Controle 8 é dedicado a logs de auditoria, estabelecendo medidas concretas como centralização, retenção mínima de 90 dias e proteção contra alterações.

Framework PPSI 2.0	Composto por um conjunto de 26 controles e 210 medidas de privacidade e segurança da informação; determina medidas como o registro de acessos a informações pessoais, a proteção desses logs e a retenção conforme prazos legais, assegurando a auditabilidade.

Fonte: elaborado pelos autores

Conforme sintetizado na Tabela 4, os principais frameworks e normas de segurança da informação e privacidade, nacionais e internacionais, oferecem diretrizes complementares para a gestão de logs. Contudo, tais documentos, embora tecnicamente robustos, não traduzem explicitamente seus requisitos em controles operacionais voltados especificamente aos logs de autenticação no âmbito das IFES, tampouco os articulam diretamente aos dez princípios da LGPD. Assim, a integração desses referenciais em um guia unificado e contextualizado não apenas atende a requisitos normativos, mas concretiza uma decisão estratégica de governança, conciliando segurança, privacidade e resiliência organizacional.

2.5 Implementação Técnica de Privacidade em Logs

A conformidade com a LGPD não se restringe à elaboração de políticas e à definição de finalidades; exige a aplicação de controles técnicos concretos sobre os dados pessoais presentes nos logs de autenticação. Esta seção detalha as principais técnicas de anonimização, pseudonimização, mascaramento e criptografia aplicáveis a esses registros, alinhando-as aos princípios da necessidade, prevenção e segurança.

2.5.1 Pseudonimização e Anonimização

Conforme definido pela LGPD (BRASIL, 2018), a pseudonimização é o tratamento por meio do qual um dado reduz a possibilidade de associação, direta ou indireta, a um indivíduo, exceto pelo uso de informação complementar. Porém, esse processo não exclui a possibilidade do dado de ser considerado pessoal. Consequentemente, os registros que contêm um identificador pseudonimizado ainda estão sujeitos a todas as obrigações da Lei, incluindo as bases legais para seu tratamento e os direitos dos titulares.

Segundo apontam Tabata e Shigeno (2024), a anonimização de dados é um processo técnico destinado a tornar razoavelmente improvável a identificação de um indivíduo a partir de um conjunto de dados, mesmo com o uso de meios indiretos. Para a LGPD (BRASIL, 2018), a anonimização trata-se da aplicação de meios técnicos razoáveis e disponíveis que eliminam a possibilidade de associação entre dado e titular. Ou seja, os dados anonimizados podem deixar de ser considerados dados pessoais, e, por consequência, são excluídos do escopo da legislação.

2.5.2 Mascaramento

O mascaramento oculta parcialmente os dados no próprio log ou em sua exibição, mantendo o valor original armazenado em ambiente controlado. É aplicado

principalmente em logs que precisam ser acessados por equipes de suporte ou análise que não exigem o dado completo. O NIST SP 800-92 (KENT; SOUPPAYA, 2006), recomenda que, sempre que possível, logs sejam consumidos por ferramentas que suportem mascaramento dinâmico, reduzindo o risco de exposição acidental.

As técnicas comuns de mascaramento incluem o modelo estático, em que o log já é gravado com o dado permanentemente oculto, impossibilitando a recuperação do valor original, sendo ideal quando não há necessidade forense. Por outro lado, o mascaramento dinâmico armazena o dado original, mas o sistema aplica a máscara apenas na consulta, com base no perfil do usuário.

2.5.3 Criptografia em Repouso e em Trânsito

A criptografia é uma medida de segurança recomendada pela LGPD e padronizada por normas como a ABNT 27002 (2022). Assim como a pseudonimização, a criptografia é mencionada pela ANPD (BRASIL, 2021) como uma técnica complementar de pseudonimização, quando combinada com a separação da chave de decodificação. Enquanto a pseudonimização atua sobre o conteúdo semântico do dado, a criptografia atua sobre sua forma de armazenamento e transmissão. Além disso, o Guia do Framework PPSI 2.0 (BRASIL, 2025) recomenda manter os logs criptografados quando armazenados por períodos superiores a 180 dias, com revisão anual das chaves de criptografia.

3. Metodologia

3.1. Natureza da Pesquisa

De acordo com Lakatos e Marconi (2017), a adequada classificação da pesquisa é elemento estruturante do delineamento metodológico, pois permite distinguir as diferentes modalidades investigativas e assegurar coerência entre problema, objetivos e procedimentos adotados. À luz desse referencial, o presente estudo caracteriza-se como qualitativo, exploratório e aplicado, desenvolvido por meio de revisão bibliográfica e análise documental de legislações, normas técnicas e frameworks de segurança e privacidade. É qualitativo na medida em que busca compreender e interpretar fenômenos complexos inseridos em contexto normativo e técnico, especificamente, a tradução de princípios jurídicos em recomendações práticas.

A classificação como pesquisa exploratória encontra respaldo em Gil (2008), para quem essa modalidade visa ampliar a familiaridade com o problema, especialmente quando há lacunas conceituais ou operacionais. No presente caso, busca-se aprofundar a compreensão acerca da tradução de requisitos legais abstratos em controles técnicos concretos aplicáveis à gestão de logs de autenticação. Trata-se, ainda, de pesquisa aplicada, pois ultrapassa a reflexão teórica e orienta-se à proposição de um artefato técnico, neste caso, um guia de referência estruturado, destinado a apoiar profissionais de TI, de segurança da informação e de privacidade na implementação de sistemas de registro de eventos de autenticação em conformidade com a LGPD.

3.2. Procedimentos Técnicos

No que se refere aos procedimentos técnicos, o estudo fundamenta-se em uma abordagem de análise documental e normativa, contemplando a seleção de legislações, normas técnicas e literatura especializada nas áreas de privacidade e cibersegurança.

A análise documental concentra-se, prioritariamente, na LGPD e no Guia do Framework de Privacidade e Segurança da Informação (PPSI), os quais constituem a base regulatória nacional. Esses documentos são complementados por normas técnicas internacionais e frameworks consolidados, permitindo integrar as exigências legais brasileiras às práticas globais de segurança da informação.

A adoção combinada desses procedimentos visa assegurar uma base teórica e normativa consistente, atualizada e tecnicamente robusta, que sustente a proposição do guia apresentado neste estudo.

3.3. Método de Análise

Para o tratamento do material coletado, adotou-se a técnica de análise de conteúdo conforme proposto por Bardin (2016), adequada à interpretação sistemática de documentos normativos e técnicos. Essa abordagem permite identificar padrões, categorias e relações relevantes para o problema investigado.

O processo analítico foi conduzido em três etapas principais: (i) pré-análise, caracterizada pela organização, leitura flutuante e seleção do material; (ii) exploração do material, com aplicação de codificação e categorização a partir dos princípios do Art. 6º da LGPD; (iii) tratamento dos resultados, envolvendo a interpretação, categorização e síntese das informações.

3.4. Critérios de Seleção Documental

Para a constituição do corpus de análise, foram definidos critérios claros de seleção documental, organizados em três categorias principais:

- Legislação**:** Lei nº 13.709/2018 (LGPD);
- Normas técnicas internacionais: Família ABNT ISO/IEC (27001:2024, 27002:2022 e 27701:2020).
- Frameworks de boas práticas: CIS Controls (Center for Internet Security, 2021) , o Guia do Framework de Privacidade e Segurança da Informação (BRASIL, 2025), NIST SP 800-92 (2006) e o OWASP Logging Cheat Sheet (2025).

3.5. Procedimento de Codificação Utilizado na Análise de Conteúdo

A exploração do material seguiu um protocolo estruturado de codificação, com categorias pré-definidas a partir dos dez princípios do art. 6º da LGPD. Foram estabelecidas regras de inclusão e exclusão para delimitar o corpus analisado: incluiu-se todo parágrafo, seção ou tabela que mencionasse direta ou indiretamente um princípio da LGPD, um controle técnico aplicável a logs de autenticação ou uma recomendação de

framework/norma relacionada à gestão de logs de autenticação sob o aspecto de privacidade; excluíram-se menções genéricas à legislação sem correlação técnica, introduções meramente protocolares e referências a normas de segurança não aplicáveis ao contexto de autenticação.

A codificação foi aplicada a um total de 8 documentos, distribuídos em três categorias: legislação (Lei 13.709/2018), resultando em 26 trechos codificados; frameworks de boas práticas (Guia PPSI 2.0; CIS Controls v8; NIST SP 800-92; OWASP Logging Cheat Sheet), com 51 trechos; e normas técnicas (ABNT 27001:2024, 27002:2022, 27701:2020), com 47 trechos. Ao todo, foram analisados 124 trechos codificados, que serviram de base para o mapeamento entre princípios da LGPD e técnicas aplicáveis apresentado na Tabela 5.

3.6 Demonstração de viabilidade Técnica

Para comprovar a viabilidade de implementação, a utilidade operacional e a eficácia das recomendações consolidadas no guia proposto, o delineamento metodológico deste estudo incorporou uma etapa de viabilidade prática por meio de experimentação técnica controlada. A inclusão de uma fase experimental em pesquisas aplicadas segundo Wohlin et al. (2024), faz-se necessário submeter artefatos teóricos ou normativos a cenários de testes práticos para avaliar sua adequação, limitações e comportamento em ambientes que emulam a realidade operacional.

Nesta perspectiva, a viabilidade foi operacionalizada utilizando uma infraestrutura de gerência centralizada de eventos do tipo Security Information and Event Management (SIEM), baseada na ferramenta de código aberto Graylog. A adoção dessa plataforma fundamenta-se em sua crescente relevância no contexto do gerenciamento centralizado de logs, especialmente em ambientes corporativos de médio e grande porte. Além disso, o Graylog destaca-se por sua capacidade de integração com diversas fontes de logs, aliada a uma interface intuitiva que facilita a criação de filtros de pesquisa, visualizações e painéis personalizados (BOSSON; MARIN, 2024).

O ambiente experimental controlado foi estruturado em quatro fases distintas e complementares:

- **Fase 1 – Configuração do Ambiente experimental:** A configuração do ambiente experimental foi implementada em uma máquina virtual (VM) utilizando o software de virtualização Oracle VM VirtualBox versão 7.0.26. A configuração da VM seguiu as seguintes especificações técnicas: Memória RAM, 4.096 MB (4 GB) alocados; Processadores, 2 núcleos virtuais; Armazenamento, Disco virtual de 64 GB (VDI); Sistema Operacional, Debian GNU/Linux (64-bit); ferramenta Graylog 4.2.13-1.
- **Fase 2 - Geração de Carga Técnica Sintética:** Com o intuito de simular o fluxo real de autenticação de um sistema de controle de acesso web de uma IFES, desenvolveu-se um script automatizado. Este script foi configurado para enviar mensagens em tempo real para o coletor (*input*) do Graylog a cada três segundos,

contendo pares de dados simulados de Cadastro de Pessoas Físicas (CPF) e endereços IP públicos gerados de forma randômica.

- **Fase 3 - Diagnóstico e Linha de Base (Baseline)**: Nesta etapa, os logs foram capturados e armazenados em texto puro, simulando o estado padrão de negligência de privacidade frequentemente encontrado em infraestruturas legadas. O resultado dessa captura bruta foi documentado e gerou o registro evidenciado na Figura 1, servindo como contraprova analítica e demonstração do descumprimento dos princípios de necessidade e prevenção da LGPD.
- **Fase 4 - Processamento e Aplicação dos Pipelines de Privacidade:** Para materializar os controles técnicos exigidos na Tabela 5, foram construídas regras de processamento e filtragem nativas dentro do SIEM, denominadas *Pipelines*. As regras foram programadas para interceptar as mensagens brutas da Fase 3 e aplicar duas transformações antes da indexação final: (i) *Pseudonimização do identificador unívoco* via função de *hash* criptográfico utilizando o algoritmo SHA-256 combinado a uma chave secreta e dinâmica do tipo *Salt* (Ex: user_hash = SHA-256(Salt + CPF)) limitado a 20 caracteres; e (ii) *Mascaramento dinâmico de conectividade*, aplicando uma expressão regular para identificar os octetos finais dos endereços IP de origem das conexões, substituindo-os pela máscara estática "XXX" (Ex: 56.45.XXX.XXX).

O resultado deste processamento automatizado gerou a massa de dados documentada na Figura 2. A análise comparativa e empírica entre os estados do log constitui o núcleo da viabilidade do Guia, permitindo avaliar se a proteção aos direitos dos titulares inviabiliza ou não a utilidade forense, a rastreabilidade e a capacidade de auditoria exigidas pelas normas codificadas.

4. Resultados e Discussão

Com base na análise de conteúdo realizada sobre a LGPD, o Guia PPSI 2.0, as normas ABNT NBR ISO/IEC 27001, 27002 e 27701, bem como o NIST SP 800-92, o CIS Controls v8 e o OWASP Logging Cheat Sheet, foi possível mapear os dez princípios previstos no art. 6º da LGPD a um conjunto de controles, técnicas e recomendações voltados à gestão de logs de autenticação. A correlação sistemática entre os requisitos legais e as boas práticas de segurança da informação permitiu consolidar o guia técnico da Tabela 5, que organiza os princípios da LGPD em categorias técnicas e recomendações operacionais para registros de autenticação, oferecendo às IFES um referencial prático para a implementação da conformidade e da proteção de dados.

Tabela 5 – Guia de Conformidade com a LGPD aplicado a Logs de Autenticação.

Princípio da LGPD	Categoria técnica	Detalhamento técnico
1. Finalidade	Definição explícita do propósito de cada log	Cada tipo de log deve ter finalidade documentada. Ex.: cumprimento de obrigação legal e execução de políticas pública. Evitar coleta genérica. Ex.: registrar apenas tentativas de login bem-sucedidas e falhas, não toda atividade do usuário.
2. Adequação	Compatibilidade entre dado coletado e finalidade	Os campos do log devem ser pertinentes ao objetivo. Ex.: registrar IP de origem é adequado para detectar acessos anômalos; registrar geolocalização pode ser excessivo e desnecessário.
3. Necessidade	Coleta mínima de dados pessoais; retenção limitada	Utilizar identificadores técnicos em vez de dados pessoais completos quando possível. Ex.: (Salt + matrícula); username, identificação única. Definir prazo de retenção compatível com a finalidade. Ex.: mínimo de 6 (seis) meses para logs de autenticação.
4. Livre Acesso	Auditoria de acesso aos logs e canal para consulta do titular	Registrar quem consultou logs com dados pessoais. Quando tecnicamente viável, oferecer canal para o titular consultar seus próprios registros de autenticação. Ex.: quando e de onde o titular acessou.
5. Qualidade dos Dados	Padronização; integridade; sincronização temporal	Usar formatos padronizados. Ex.: JSON, CEF; sincronizar relógios via NTP; aplicar checksum, hash ou assinatura digital para detectar alterações não autorizadas. Ex.: timestamp em UTC conforme ABNT NBR ISO 8601-1 (2022) 2025-04-26T20:28:10Z;
6. Transparência	Documentação da política de logs; auditoria de acessos	Divulgar política de logs. Ex.: o que é registrado, por quanto tempo, finalidade; exibir aviso no momento do login. Ex.: o sistema deve exibir ou enviar ao titular a data e a hora do seu login anterior bem-sucedido, bem como os detalhes de quaisquer tentativas de autenticação do titular.
7. Segurança	Criptografia; controle de acesso; segregação; gestão de chaves	Criptografia dos logs de autenticação em repouso e em trânsito. Ex.: TLS 1.3, AES-256-GCM; controle de acesso baseado em papéis. Ex.:RBAC; ambiente segregado e restringir acesso apenas a pessoal autorizado.
8. Prevenção	Mascaramento; pseudonimização; Supressão de dados sensíveis;	Aplicar pseudonimização em identificadores. Ex.: user_hash = SHA-256(Salt + matrícula); mascarar dinamicamente IP para geração de relatórios. Ex.:192.168.xxx.xxx; manter chaves de reversão em cofre seguro.
9. Não Discriminação	Supressão de dados sensíveis; mascaramento dinâmico	Sempre que possível, evitar o registro de dados pessoais sensíveis em logs de autenticação, limitando a coleta ao estritamente necessário para finalidades legítimas de segurança. Obs.: caso a IFES utilize registros de autenticação envolvendo DPS, recomenda-se implementar controles técnicos de supressão, mascaramento, pseudonimização ou segregação de acesso aos campos classificados como DPS.
10. Responsabilização	Documentação; auditoria contínua; análise automatizada	Manter registros das configurações de log, das técnicas aplicadas e dos acessos aos logs. Recomenda-se realizar auditoria periódica para verificar conformidade com este guia.

Fonte: Elaborado pelos autores

A Tabela 5 evidencia que a gestão de logs de autenticação alinhada à LGPD não é um obstáculo intransponível, mas sim uma oportunidade de amadurecimento dos processos de segurança da informação. Conforme estabelecido na fundamentação teórica, ABNT 27002 (2022), NIST SP 800-92 (KENT e SOUPPAYA, 2006) e PPSI 2.0 já previam medidas como pseudonimização, criptografia e controle de acesso que, quando aplicados, atendem simultaneamente aos princípios de segurança e aos princípios da LGPD.

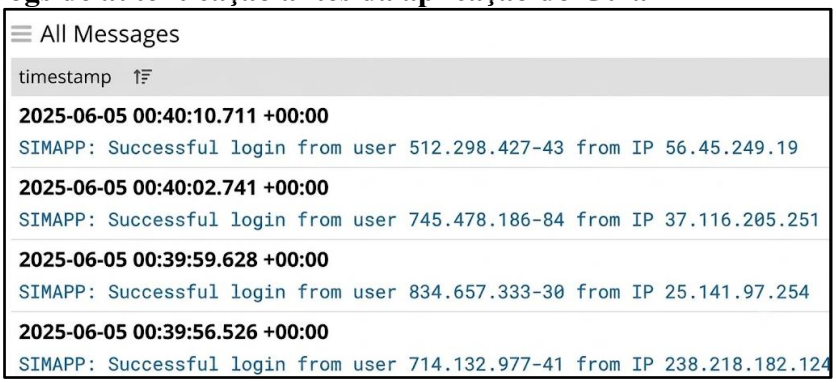
Na Tabela 5, nota-se que o princípio da finalidade funciona como um guia para os princípios da adequação e da necessidade. Isso significa que, sem uma finalidade clara e legítima, não é possível avaliar se o tratamento de dados é realmente adequado àquela finalidade nem se os dados coletados são estritamente necessários. Portanto, quando a finalidade é falha ou mal definida, fica comprometida a proteção de dados pessoais, pois a adequação e a necessidade perdem sua base de referência.

Nesse cenário, a definição de uma base legal adequada torna-se elemento central para a legitimidade do tratamento. No âmbito das IFES, a coleta e o armazenamento de logs de autenticação encontram respaldo prioritário no Art. 23 da LGPD (BRASIL, 2018), que disciplina o tratamento de dados pela administração pública, vinculando-o às finalidades de execução de políticas públicas e ao interesse público.

De forma complementar, o Art. 7º, inciso II, cumprimento de obrigação legal, e inciso III, execução de políticas públicas, justificam o registro de eventos de autenticação como parte das medidas de segurança da informação exigidas por normativos nacionais, dentre os quais se destacam o Decreto nº 9.637/2018 (BRASIL, 2018), que institui Política Nacional de Segurança da Informação, a Norma Complementar nº 21 do GSI/PR (2014b) e a Lei nº 12.965/2014 (BRASIL,2014a).

Para demonstrar a viabilidade prática das técnicas recomendadas na Tabela 5, apresentam-se dois registros de autenticação antes e depois da aplicação de medidas de pseudonimização e mascaramento. A Figura 1 exibe a coleta de logs da ferramenta SIEM Graylog, em tempo real, dos logs criados pelo script gerador de acesso típicos de logs gerados por um sistema de controle de acesso web, com CPF e IP randômicos a cada três segundos. A Figura 2 demonstra o mesmo conjunto de informações após a aplicação da Tabela 5 com as técnicas de pseudonimização e mascaramento dinâmico de IP.

Figura 1 – logs de autenticação antes da aplicação do Guia



Fonte: Elaborado pelos autores

Figura 2 –Logs de autenticação após a aplicação da pseudonimização e do mascaramento

Fonte: Elaborado pelos autores

As Figuras 1 e 2 evidenciam, de forma empírica, que a aplicação das recomendações propostas neste guia permite compatibilizar requisitos de segurança da informação com as exigências de proteção de dados estabelecidas pela LGPD. Enquanto a Figura 1 representa um cenário típico de coleta de logs em texto claro, no qual informações como CPF e endereço IP são armazenadas integralmente, ampliando os riscos de exposição indevida e contrariando os princípios da necessidade e da adequação (CANEDO et al., 2022). Na Figura 2, o log resultante processado pelas regras de pipeline do Graylog evidencia que a desidentificação e o mascaramento executados mantêm a sequência temporal dos eventos e a distinção precisa de sessões concorrentes. Dessa forma, reduzem a superfície de exposição sem anular os alertas contra ataques de força bruta ou intrusões na rede das IFES.

Esses resultados reforçam que a adoção de técnicas de engenharia de privacidade não compromete a utilidade operacional dos logs de autenticação. Ao contrário, demonstra que mecanismos como pseudonimização, mascaramento e segregação de acesso possibilitam atender simultaneamente aos requisitos de segurança da informação, auditoria e conformidade regulatória, corroborando a perspectiva de que privacidade e segurança constituem objetivos complementares e não conflitantes.

5. Considerações Finais

Os resultados obtidos permitiram atingir o objetivo proposto de desenvolver um guia técnico para a gestão de logs de autenticação em Instituições Federais de Ensino Superior (IFES) em conformidade com a LGPD. A partir da análise integrada da legislação brasileira, das normas técnicas ABNT NBR ISO/IEC 27001, 27002 e 27701, do NIST SP 800-92 e do Framework PPSI 2.0, foi possível estruturar um conjunto de recomendações que traduz os dez princípios previstos no art. 6º da LGPD em controles técnicos aplicáveis à gestão de registros de autenticação.

A principal contribuição deste trabalho consiste na operacionalização de princípios legais abstratos em mecanismos concretos de engenharia de privacidade voltados à infraestrutura de tecnologia da informação. Ao propor diretrizes objetivas para o tratamento de logs de autenticação, a pesquisa demonstra que é possível conciliar os

requisitos de segurança da informação com as exigências da LGPD, preservando a capacidade de investigação e resposta a incidentes sem comprometer a privacidade dos titulares dos dados.

Embora as técnicas propostas tenham sido validadas experimentalmente em ambiente controlado utilizando o SIEM Graylog, evidenciando sua viabilidade técnica e a manutenção da utilidade dos registros para fins forenses, o Guia ainda não foi implementado em larga escala integrado aos processos de governança de uma IFES. Além disso, o estudo concentrou-se exclusivamente nos logs de autenticação, não abrangendo outras categorias de registros que também possuem relevância para a gestão da segurança da informação.

Como perspectivas para trabalhos futuros, recomenda-se a implementação do guia em ambiente de produção para avaliar aspectos como desempenho e escalabilidade dos pipelines de processamento em cenários com grande volume de eventos, bem como a ampliação da abordagem para logs de bancos de dados, aplicações e serviços em nuvem governamental. Também se destacam como oportunidades de continuidade o desenvolvimento de mecanismos automatizados de auditoria voltados à verificação de conformidade com a LGPD e as orientações da ANPD.

Conclui-se, portanto, que a proteção da privacidade não deve ser compreendida como uma restrição às atividades de segurança da informação, mas como uma oportunidade de amadurecimento da governança digital moderna. Ao demonstrar que é possível preservar a capacidade de auditoria, a resposta a incidentes e a rastreabilidade dos eventos sem expor desnecessariamente dados pessoais, este trabalho contribui para aproximar os requisitos legais da LGPD das práticas operacionais de gestão de logs de autenticação, oferecendo às IFES um modelo tecnicamente viável para conciliar conformidade regulatória, resiliência cibernética e proteção dos direitos fundamentais dos titulares dos dados.

6. Referências

ARAÚJO, Aletéia P. F.; COSTA, Breno; BACHIEGA JR., Joao; CARVALHO, Leonardo R.; BUYYA, Rajkumar. Observability in Fog Computing. 2024. DOI: 10.48550/arXiv.2411.17753. Disponível em: https://www.researchgate.net/publication/386211074_Observability_in_Fog_Computing. Acesso em: 15 jan. 2026.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 27001:2022/Emenda 1:2024: Segurança da informação, segurança cibernética e proteção à privacidade — Sistemas de gestão da segurança da informação — Requisitos. Rio de Janeiro: ABNT, 2024.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27701:2019 versão corrigida 2020**: 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, 2020. 82 p. ISBN 978-85-07-08404-4.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27557:2023**: Segurança da informação, segurança cibernética e proteção à privacidade — Diretrizes para gestão de riscos de privacidade organizacional. Rio de Janeiro: ABNT, 2023.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27002:2022**: Segurança da informação, segurança cibernética e proteção à privacidade - Controles de segurança da informação. 3. ed. Rio de Janeiro: ABNT, 2022. 191 p.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 8601-1:2022**: Data e hora - Representação para intercâmbio de informação -Parte 1: Requisitos básicos. Rio de Janeiro: ABNT, 2022. 36 p.

BARDIN, Laurence. *Análise de Conteúdo*. Tradução: Luís Antero Reto, Augusto Pinheiro. São Paulo: Edições 70, 2016. 280 p. ISBN 978-85-62938-04-7.

BASSO, Douglas Eduardo; MARIN, Luciano Heitor Gallegos. ANÁLISE COMPARATIVA DE SOLUÇÕES DE CÓDIGO ABERTO DE GERENCIAMENTO DE EVENTOS E SEGURANÇA DA INFORMAÇÃO. **REVISTA FOCO**, v. 17, n. 12, p. e7368-e7368, 2024.

BRASIL. Gabinete de Segurança Institucional da Presidência da República. **Norma Complementar nº 21/IN01/DSIC/GSIPR**: Estabelece Diretrizes para Gestão de Logs no âmbito da Administração Pública Federal, direta e indireta. Brasília: GSI/PR, 2014b. Disponível em: https://www.gov.br/gsi/pt-br/seguranca-da-informacao-e-cibernetica/legislacao/NC21.pdf . Acesso em: 21 abr. 2026.

BRASIL. **Decreto nº 9.637, de 26 de dezembro de 2018**. Institui a Política Nacional de Segurança da Informação. Brasília, DF: Presidente da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/d9637.htm. Acesso em: 9 abril 2026.

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: Presidente da República, 2014a. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 9 abril 2026.

BRASIL. Gabinete de Segurança Institucional da Presidência da República. Guia do Framework de Privacidade e Segurança da Informação (PPSI) 2.0. Brasília, DF: GSI, 2025. Disponível em: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi-2.0/arquivos/guiafwppsi2-0-v1-2-30012026.pdf. Acesso em: 15 mar. 2026.

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

BRASIL. Autoridade Nacional de Proteção de Dados. **Guia Orientativo sobre Segurança da Informação para Agentes de Tratamento de Pequeno Porte**. Versão 1.0. [S. l.]: ANPD, out. 2021. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia_seguranca_da_informacao_para_atpps___defeso_eleitoral.pdf/@@display-file/file . Acesso em: 19 abril 2026.

CENTER FOR INTERNET SECURITY. CIS critical security controls: version 8. 2021. Disponível em: https://www.cisecurity.org/controls/v8. Acesso em: 2 abril 2026.

CHUVAKIN, Anton; SCHMIDT, Kevin; PHILLIPS, Christopher. **Logging and Log Management**: The Authoritative Guide to Understanding the Concepts Surrounding Logging and Log Management. 1. ed. Waltham, MA: Syngress, 2012. Disponível em: https://www.oreilly.com/library/view/logging-andlog/9781597496353/xhtml/Copyright.html. Acesso em: 21 abr. 2026.

CANEDO, Edna Dias et al. Guidelines adopted by agile teams in privacy requirements elicitation after the Brazilian general data protection law (LGPD) implementation. **Requirements Engineering**, v. 27, n. 4, p. 545-567, 2022.

OWASP FOUNDATION. **Logging Cheat Sheet**. [S. l.]: OWASP, [2025]. Disponível em: https://cheatsheetseries.owasp.org/cheatsheets/Logging_Cheat_Sheet.html. Acesso em: 1 mar. 2026.

GIL, Antonio Carlos. *Métodos e Técnicas de Pesquisa Social*. 6. ed. São Paulo: Atlas, 2008.

KENT, Karen; SOUPPAYA, Murugiah. Guide to computer security log management. **NIST special publication**, v. 92, p. 1-72, 2006.

KUNIMOTO, Michio; OKUBO, Takao. Analysis and consideration of detection methods to prevent fraudulent access by utilizing attribute information and the access log history. **Journal of Information Processing**, v. 31, p. 602-608, 2023.

LAKATOS, Eva Maria; MARCONI, Marina de Andrade. *Metodologia Científica*. 7. ed. São Paulo: Atlas, 2017.

PEIXOTO, Mariana et al. The perspective of Brazilian software developers on data privacy. **Journal of Systems and Software**, v. 195, p. 111523, 2023.

ROCHA, Lucas Dalle; SILVA, Geovana Ramos Sousa; DIAS CANEDO, Edna. Privacy compliance in software development: A guide to implementing the LGPD principles.

In: **Proceedings of the 38th ACM/SIGAPP Symposium on Applied Computing**. 2023. p. 1352-1361.

ROCHA, Lucas Dalle; CANEDO, Edna Dias. Optimizing compliance: Comparative study of data laws and privacy frameworks. 2025.

TABATA, N.; SHIGENO, M. **Application of Data Anonymization to Smartphone Apps Usage Logs**. In: INTERNATIONAL CONFERENCE ON BIG DATA ANALYTICS (ICBDA), 9., 2024. **Anais** [...]. [S. l.]: IEEE, 2024. p. 1-10. Disponível em: https://ieeexplore.ieee.org/document/10607298. Acesso em: 3 abril 2026.

VILELA, Ederson Mendes. **Sistema para guarda de logs de acesso baseado no Marco Civil da Internet**. 2017.

WOHLIN, Claes et al. Experimentation in Software Engineering (2024 edition). 2024.