

Análise de conformidade das normas de segurança da informação de uma organização militar do Exército Brasileiro à luz da ISO 31000:2018, da ABNT NBR 23894:2023 e do NIST Risk Management Framework

Compliance analysis of information security standards of a Brazilian Army military organization in the light of ISO 31000:2018, ABNT NBR 23894:2023 and NIST Risk Management Framework

Análisis de conformidad de las normas de seguridad de la información de una organización militar del Ejército Brasileño a la luz de la ISO 31000:2018, ABNT NBR 23894:2023 y el NIST Risk Management Framework

Marcelo Zulian Hanna

Especialista em Privacidade e Segurança da Informação (em formação)

Instituição: Universidade de Brasília (UNB)

Endereço: Brasília - Distrito Federal, Brasil

E-mail: marcelozulianhanna@gmail.com

João Souza Neto

Pós-Doutor em Segurança Cibernética

Instituição: Universidade de Brasília (UNB)

Endereço: Brasília - Distrito Federal, Brasil

E-mail: neto.joao@unb.br

RESUMO

Este artigo analisa a conformidade das normas de segurança da informação de uma Organização Militar de Ensino (OME) do Exército Brasileiro com a ISO 31000:2018, a ABNT NBR 23894:2023 e o NIST Risk Management Framework (NIST SP 800-37), incorporando ainda a dimensão jurídica da Lei de Acesso à Informação (LAI, Lei nº 12.527/2011) e da Lei Geral de Proteção de Dados Pessoais (LGPD, Lei nº 13.709/2018). A pesquisa é documental e comparativa, com gap analysis aplicado ao conjunto de instrumentos normativos de acesso não restrito em vigor na organização, Política Geral de Segurança da Informação, Plano de Gestão de Riscos 2024–2027 e instrumentos complementares. Os resultados mostram que a

organização dispõe de estrutura normativa sólida e mais abrangente do que as Instruções Gerais para a Salvaguarda de Assuntos Sigilosos isoladas sugerem, com seis oportunidades de aprimoramento identificadas: necessidade de integração formal entre frameworks de gestão de riscos; oportunidade de retroalimentação documental entre auditorias e plano de riscos; possibilidade de ampliar o contexto organizacional para contemplar o perfil de ensino e as obrigações da LGPD quanto a dados de menores; oportunidade de consolidação entre o plano de riscos de TI e o institucional; necessidade de formalização do processo de autorização e registro de risco residual; e necessidade de estruturação de mapeamento de dados pessoais e mecanismo de transparência ativa em conformidade com a LAI. Identifica-se ainda oportunidade de antecipação de riscos relativos à Inteligência Artificial, à luz da ABNT NBR 23894:2023. Propõem-se sete adaptações priorizadas.

Palavras-chave: gestão de riscos; segurança da informação; ISO 31000:2018; ABNT NBR 23894:2023; NIST RMF; Lei de Acesso à Informação; LGPD; organização militar de ensino; gap analysis.

ABSTRACT

This article analyzes the compliance of the information security standards of a Brazilian Army Military Teaching Organization (MTO) with ISO 31000:2018, ABNT NBR 23894:2023, and the NIST Risk Management Framework (NIST SP 800-37), additionally incorporating the legal dimension of the Access to Information Act (LAI, Law No. 12,527/2011) and the General Personal Data Protection Law (LGPD, Law No. 13,709/2018). The research is documentary and comparative, applying gap analysis to the set of unrestricted normative instruments in force in the organization. Results show the organization has a robust and advanced normative structure, with six improvement opportunities identified: need for formal integration between risk management frameworks; opportunity for documentary feedback between audits and the risk plan; possibility of broadening the organizational context to address the teaching profile and LGPD obligations regarding minors data; opportunity for consolidation between the IT risk plan and the institutional plan; need to formalize the authorization and residual risk acceptance process; and need to structure personal data flow mapping and active transparency mechanisms in compliance with LAI. An opportunity to anticipate risks related to Artificial Intelligence is also identified. Seven prioritized adaptations are proposed.

Keywords: risk management; information security; ISO 31000:2018; ABNT NBR 23894:2023; NIST RMF; Access to Information Act; LGPD; military teaching organization; gap analysis.

RESUMEN

Este artículo analiza la conformidad de las normas de seguridad de la información de una Organización Militar de Enseñanza del Ejército Brasileño con la ISO 31000:2018, la ABNT NBR 23894:2023 y el NIST Risk Management Framework, incorporando además la dimensión jurídica de la Ley de Acceso a la Información (LAI) y la Ley General de Protección de Datos Personales (LGPD). La investigación es documental y comparativa. Los resultados muestran una estructura normativa sólida con seis oportunidades de mejora identificadas, incluyendo la necesidad de mapeo de flujo de datos personales y mecanismos de transparencia activa, y oportunidades de anticipación de riesgos relacionados con la Inteligencia Artificial. Se proponen siete adaptaciones priorizadas.

Palabras clave: gestión de riesgos; seguridad de la información; ISO 31000:2018; ABNT NBR 23894:2023; NIST RMF; Ley de Acceso a la Información; LGPD; organización militar de enseñanza; análisis de brechas.

1 INTRODUÇÃO

A segurança da informação integra a rotina organizacional de praticamente todas as forças armadas do mundo. No Exército Brasileiro, essa tradição encontra amparo normativo nas Instruções Gerais para a Salvaguarda de Assuntos Sigilosos, EB10-IG-01.011, norma voltada primordialmente ao aspecto de confidencialidade, apenas um dos três pilares da tríade CIA (confidencialidade, integridade e disponibilidade), cujo histórico regulatório remonta ao Decreto nº 79.099/1977. Cinco movimentos recentes tornaram oportuna uma revisão e atualização desse arcabouço sob a ótica da gestão de risco: (1) a consolidação da ISO 31000:2018 como referência internacional de gestão de riscos; (2) a publicação da ABNT NBR 23894:2023 sobre gestão de riscos em Inteligência Artificial; (3) a adoção crescente do NIST Risk Management Framework por governos e forças armadas ao redor do mundo; (4) a entrada em vigor da Lei Geral de Proteção de Dados Pessoais (LGPD, Lei nº 13.709/2018), que estabelece obrigações de segurança e responsabilização no tratamento de dados pessoais por entidades públicas; e (5) a maturação da aplicação da Lei de Acesso à Informação (LAI, Lei nº

12.527/2011) na administração pública federal, que estabelece o princípio da publicidade como regra e o sigilo como exceção, demandando que decisões sobre gestão de riscos sejam documentadas e rastreáveis.

A organização objeto deste estudo é uma Organização Militar de Ensino do Exército Brasileiro, com a atribuição de promover educação básica nos níveis fundamental II e médio. Esse perfil determina um contexto informacional específico: dados de militares, servidores civis e alunos, incluindo menores de idade, convivem no mesmo ambiente com informações administrativas e operacionais, cada qual com requisitos de proteção distintos. A natureza educacional cria oportunidades de alinhamento normativo adicionais em relação às demais organizações militares: a LGPD confere proteção especial aos dados pessoais de crianças e adolescentes (art. 14), recomendando atenção ao consentimento dos responsáveis e à minimização no tratamento; a LAI orienta a transparência ativa de atos administrativos, salvo exceções taxativamente previstas; e a combinação dos dois regimes, publicidade por padrão (LAI) e proteção reforçada de dados pessoais (LGPD), representa um equilíbrio a ser gerido formalmente, tal como ocorre nas instituições federais de ensino e universidades públicas brasileiras.

Cabe destacar que a organização analisada se preocupa com o assunto desde longa data, tanto por imposição do escalão superior quanto por exigências governamentais. Em fevereiro de 2026, foram aprovados a Política Geral de Segurança da Informação (PSI), alinhada à ISO 27001, e o Plano de Gestão de Riscos 2024–2027, que cita explicitamente a ABNT NBR ISO 31000:2018. Uma oportunidade de aprimoramento identificada neste trabalho é a incorporação formal da LGPD e da LAI como referenciais de conformidade nos instrumentos normativos existentes, passo natural para uma organização que já demonstra maturidade em gestão de riscos e que trata dados pessoais de menores. A pergunta que orienta este trabalho é: em que medida o arcabouço normativo de segurança da informação da organização atende à ISO 31000:2018, à ABNT NBR 23894:2023, ao NIST RMF, à LGPD e à LAI, e quais aprimoramentos adicionais podem ser propostos?

1.1 OBJETIVOS

O objetivo geral é analisar a conformidade das normas de segurança da informação da organização com os referenciais adotados, identificar as lacunas existentes e propor adaptações

concretas. Os objetivos específicos são: (a) mapear os instrumentos normativos em vigor; (b) realizar gap analysis comparando esses instrumentos com a ISO 31000:2018 e o NIST RMF; (c) identificar riscos emergentes de Inteligência Artificial nos termos da ABNT NBR 23894:2023; (d) formular adaptações normativas viáveis; e (e) avaliar a aderência do arcabouço normativo às obrigações legais da LGPD e da LAI, identificando lacunas de conformidade jurídica.

Este artigo está organizado em seis seções. A seção 2 apresenta o referencial teórico, abordando a ISO 31000:2018, o NIST Risk Management Framework, a ABNT NBR 23894:2023 e o regime jurídico da LAI e da LGPD aplicado a OMEs. A seção 3 descreve a metodologia adotada. A seção 4 apresenta a análise e os resultados do gap analysis, incluindo avaliação de conformidade com LGPD e LAI. A seção 5 formula as sete propostas de adaptações. A seção 6 traz as conclusões.

2 REFERENCIAL TEÓRICO

A ISO 31000:2018 é a norma internacional de gestão de riscos, não certificável, aplicável a qualquer tipo de organização. Organiza-se em três componentes: princípios, estrutura e processo. Os princípios definem as características que a gestão de riscos deve ter; a estrutura define como ela se integra à governança, num estrutura de melhoria contínua; o processo operacionaliza as etapas de comunicação, contexto, avaliação de riscos, tratamento, monitoramento e registro.

A etapa de tratamento (cláusula 6.5) é a que responde à pergunta central deste trabalho: como se decide implantar um controle de segurança? A norma determina que a decisão deve equilibrar custos e benefícios, considerar requisitos legais e documentar o risco residual aceito. A ABNT NBR 16337:2020 é a versão brasileira, com conteúdo técnico idêntico.

A seleção das opções de tratamento do risco deve equilibrar os benefícios potenciais em relação aos custos potenciais e considerar os requisitos legais, regulatórios e outros (ISO 31000, 2018, cláusula 6.5.2, tradução nossa).

O NIST Risk Management Framework (NIST SP 800-37, Rev. 2) organiza a gestão de riscos em sete etapas: Preparação, Categorização, Seleção de controles, Implementação, Avaliação, Autorização e Monitoramento. A etapa de Autorização, decisão formal da autoridade competente sobre aceitação do risco residual, é a que mais diretamente responde à

pergunta central deste trabalho, criando rastreabilidade e responsabilização que frameworks prescritivos tradicionais não garantem.

No contexto do Exército Brasileiro, a Diretriz Estratégica de Inteligência Artificial, EB20-D02.031 (Portaria EME/C Ex nº 1.318/2024), classifica os sistemas de IA militares em três categorias de risco e determina que o controle decisório permaneça sob julgamento humano, alinhamento direto com a ABNT NBR 23894:2023.

A literatura científica sobre avaliação de conformidade normativa em organizações de ensino ainda é incipiente, em contraste com a vasta produção voltada a ambientes corporativos e governamentais. Lima et al. (2022), em estudo comparativo sobre a adoção de frameworks de segurança em organizações públicas brasileiras, demonstraram que a metodologia de gap analysis com escala qualitativa de conformidade, classificando requisitos em plenamente atendido, parcialmente atendido ou não explicitado, permite identificar lacunas com precisão suficiente para orientar planos de adequação. Esse modelo metodológico informa a estrutura analítica adotada neste trabalho.

A ABNT NBR 23894:2023 aplica os princípios da ISO 31000 ao ciclo de vida de sistemas de Inteligência Artificial. Ela identifica riscos específicos: viés algorítmico, opacidade dos modelos, vulnerabilidades a ataques adversariais e riscos à privacidade. Exige integração desses riscos ao processo geral de gestão, cobrindo desenvolvimento, operação e descontinuação dos sistemas.

Lei de Acesso à Informação e Lei Geral de Proteção de Dados Pessoais

A Lei de Acesso à Informação (LAI, Lei nº 12.527/2011), regulamentada pelo Decreto nº 7.724/2012, estabelece que toda informação produzida ou custodiada pelo poder público é pública por natureza, sendo o sigilo a exceção e não a regra. O art. 6º impõe à administração pública a obrigação de garantir a proteção da informação sigilosa e pessoal, o que cria um ponto de contato direto com a gestão de riscos em segurança da informação: a decisão sobre o que é sigiloso, por quanto tempo e com qual justificativa precisa ser documentada, rastreável e defensável perante qualquer pedido de transparência. Nesse sentido, a etapa de Autorização do NIST RMF, que exige que uma autoridade formalmente designada documente a aceitação do risco residual, é também a etapa que confere rastreabilidade decisória compatível com a LAI: sem ela, a organização não consegue demonstrar, em eventual pedido de acesso à informação, por que determinada decisão de segurança foi tomada, por quem e com qual base técnica.

A Lei Geral de Proteção de Dados Pessoais (LGPD, Lei nº 13.709/2018) impõe um regime de obrigações de segurança sobre o tratamento de dados pessoais que vai além das normas de segurança da informação tradicionais. Seus princípios (art. 6º), finalidade, adequação, necessidade, livre acesso, qualidade, transparência, segurança, prevenção, não discriminação e responsabilização, traduzem-se em requisitos concretos para a gestão de riscos: a organização deve tratar apenas os dados estritamente necessários (necessidade), implementar medidas técnicas e administrativas aptas a protegê-los (segurança), adotar postura proativa de mitigação de danos (prevenção) e demonstrar o cumprimento dessas obrigações (responsabilização e prestação de contas). Para entidades públicas, o art. 23 determina que o tratamento seja realizado para o atendimento de sua finalidade pública e em conformidade com o interesse público. O art. 37 exige a elaboração de Relatório de Impacto à Proteção de Dados Pessoais (RIPD) quando o tratamento puder gerar riscos às liberdades civis e aos direitos fundamentais dos titulares, o que é especialmente relevante para OMEs, cujo universo de dados inclui menores de idade.

Para as Organizações Militares de Ensino, a proteção especial conferida pelo art. 14 da LGPD aos dados de crianças e adolescentes constitui obrigação de gestão de riscos autônoma: o tratamento desses dados deve ser realizado no melhor interesse do menor, com coleta mínima de dados e mecanismos que possibilitem a responsáveis legais o exercício dos direitos previstos na lei. A dificuldade de mapeamento de fluxo de dados pessoais (data mapping) impede a totalidade de identificação de trânsito dos dados das pessoas, por quanto tempo e com quais controles, condição prévia indispensável para qualquer avaliação de risco compatível com a LGPD. Além disso, as entidades públicas devem indicar Encarregado pelo Tratamento de Dados Pessoais (DPO), conforme art. 41 da LGPD, e comunicar à Autoridade Nacional de Proteção de Dados (ANPD) a ocorrência de incidentes de segurança que possam acarretar risco ou dano relevante aos titulares (art. 48), criando obrigação de resposta a incidentes que precisa estar integrada ao processo de gestão de riscos existente.

A tensão entre LAI e LGPD é estrutural e precisa ser gerenciada: a LAI presume publicidade; a LGPD impõe restrições ao acesso a dados pessoais. No contexto de uma OME, isso significa que registros acadêmicos, fichas de saúde e dados cadastrais de alunos menores estão protegidos pela LGPD (acesso restrito), enquanto atos administrativos, contratos e estrutura organizacional estão sujeitos à transparência ativa da LAI. A matriz de riscos da organização precisa contemplar essa dualidade: risco de exposição indevida de dados pessoais

(violação da LGPD) e risco de ocultação indevida de informação pública (violação da LAI) são igualmente relevantes e exigem controles distintos.

3 METODOLOGIA

A pesquisa é qualitativa e descritiva, de natureza aplicada (GIL, 2017). O método é a pesquisa documental com análise comparativa estruturada na forma de gap analysis, técnica amplamente utilizada em estudos de conformidade normativa para identificar lacunas entre o estado atual de uma organização e os requisitos de normas de referência (CALDER; WATKINS, 2019). Todos os documentos utilizados são de acesso não restrito.

As fontes primárias são: (a) Política Geral de Segurança da Informação, PSI versão 1.1, fevereiro de 2026, com Anexos A a G; (b) Plano de Gestão de Riscos 2024–2027, 3ª Edição, com Matriz de Riscos e Controle; (c) Plano Diretor de Tecnologia da Informação 2024–2027; (d) Plano de Auditoria de TI, versão 1.2/2026; (e) IGSAS EB10-IG-01.011, 1ª Edição, 2014; (f) ISO 31000:2018, ABNT NBR 16337:2020 e ABNT NBR 23894:2023; (g) NIST SP 800-37, Rev. 2, 2018; e (h) legislação federal aplicável: Lei nº 12.527/2011 (LAI), Decreto nº 7.724/2012 (regulamentação da LAI) e Lei nº 13.709/2018 (LGPD). A inclusão das duas últimas leis como fontes de análise responde à ausência de referência a elas nos documentos internos da organização, o que por si só constitui dado relevante para o gap analysis.

O gap analysis foi conduzido em quatro etapas: (1) levantamento dos requisitos da ISO 31000:2018, da ABNT NBR 23894:2023, do NIST RMF, da LAI e da LGPD; (2) verificação do atendimento pelos documentos internos, classificado em atendido plenamente (AP), atendido parcialmente (AT) ou não explicitado (NE), conforme metodologia de Lima et al. (2022); (3) identificação de lacunas de conformidade normativa e jurídica; e (4) organização dos resultados em matrizes de lacunas com adaptações priorizadas por grau de urgência e esforço de implementação. As limitações incluem observação em uma única organização, análise restrita a documentos de acesso não restrito e impossibilidade de verificar práticas informais.

4 ANÁLISE E RESULTADOS

4.1 Arcabouço normativo da organização analisada

A organização dispõe de conjunto normativo que vai bem além das IGSAS. A PSI (fevereiro de 2026), alinhada à ISO 27001, constitui o Comitê de Gestão de Segurança da Informação (CGSI), presidido pelo Subcomandante, com responsabilidades em três níveis. O Plano de Gestão de Riscos cita explicitamente a ABNT NBR ISO 31000:2018 e dispõe de Matriz de Riscos com avaliação de probabilidade e impacto. O Plano de Auditoria de TI define processo estruturado em sete etapas. A trajetória histórica está registrada: metas de 15% de implantação da gestão de risco em maio de 2023 e 40% em novembro do mesmo ano. Uma oportunidade de evolução identificada é a incorporação formal da LGPD e da LAI como referenciais de conformidade no arcabouço existente, alinhamento natural com o estágio de maturidade já demonstrado pela organização.

4.2 Convergências com os referenciais adotados

Cinco convergências merecem registro. Primeiro: referência explícita à ISO 31000:2018 no Plano de Gestão de Riscos. Segundo: Matriz de Riscos com avaliação de probabilidade e impacto, correspondendo às cláusulas 6.4.3 e 6.4.4 da ISO 31000 e à etapa de Categorização do NIST RMF. Terceiro: CGSI formalmente constituído, componente de liderança e comprometimento da ISO 31000 (cláusula 5.2). Quarto: Plano de Auditoria de TI com etapas estruturadas de análise de riscos, coleta de evidências e acompanhamento de recomendações. Quinto: analogia direta entre a classificação das IGSAS (Reservado, Secreto, Ultrassecreto) e a categorização do NIST RMF (impacto baixo, moderado e alto).

4.3 Gap analysis: lacunas identificadas

Nº	Requisito	Status	Evidência	Recomendação
1	Integração PSI/CGSI ↔ Plano de Gestão de Riscos, ISO 31000, cl. 5.3	Parcial	PSI: ISO 27001; Plano: ISO 31000. Sem procedimento formal de integração	Procedimento CGSI ↔ EGP com critérios de relevância estratégica

Nº	Requisito	Status	Evidência	Recomendação
2	Retroalimentação auditorias → Plano, ISO 31000, cl. 5.6–5.7; NIST Monitoramento	Parcial	Auditorias robustas, sem mecanismo formal de retroalimentação com registro de risco residual	Campo de risco residual nos formulários e reunião semestral de revisão
3	Contexto de organização de ensino, ISO 31000, cl. 6.3; NIST Preparação	Parcial	Plano mapeia 30 processos, sem partes interessadas externas do ambiente de ensino	Ampliar Anexo A com famílias, parceiros acadêmicos e ameaças do contexto educacional
4	Integração plano TI ↔ Plano institucional, ISO 31000, cl. 5.3; NIST Categorização	Parcial	Mesma equipe técnica, sem consolidação periódica formal	Processo semestral Chefe Sec Infor ↔ EGP documentado em ata
5	Autorização formal e aceitação de risco residual, NIST Autorização; ISO 31000, cl. 6.5.3	Não explicitado	Sem procedimento que documente decisão de aceitar risco residual com autoridade designada	Processo de autorização formal com designação de autoridade, registro e prazo de validade

Tabela 1. Gap analysis: aderência à ISO 31000:2018 e ao NIST RMF.

Oportunidade 1 - Integração: os dois frameworks coexistem com oportunidade de articulação formal. Uma ocorrência identificada pelo CGSI pode não constar automaticamente do Plano de Gestão de Riscos; da mesma forma, um risco estratégico do plano pode se beneficiar de revisão pelo CGSI. A estruturação de fluxo formal entre os dois instrumentos fortaleceria a coerência do sistema de gestão de riscos.

Oportunidade 2 - Processo: os instrumentos de auditoria são bem estruturados, sendo recomendável o estabelecimento de mecanismo formal que devolva os achados ao Plano de Gestão de Riscos. A ISO 31000 (cl. 5.7) e o NIST RMF (etapa Monitoramento) convergem nesse ponto: o fechamento documentado do ciclo fortalece a rastreabilidade e a melhoria contínua.

Oportunidade 3 - Escopo: o contexto específico do ambiente de ensino, alunos menores, famílias, parceiros acadêmicos, pode ser mais explicitamente contemplado como fator de risco na Matriz de Riscos, em linha com a cláusula 6.3 da ISO 31000 e a etapa de Preparação do NIST RMF. No âmbito da LGPD, instrumentos como o mapeamento de fluxo de dados (data mapping), a indicação de Encarregado (DPO) e o Relatório de Impacto à Proteção de Dados (RIPD) representam etapas recomendadas para entidades públicas que tratem dados pessoais de menores, e sua implementação estruturaria formalmente práticas de proteção que a organização já realiza de fato.

Oportunidade 4 - Articulação: o Plano Diretor de TI e o Plano de Gestão de Riscos foram elaborados pela mesma equipe técnica, o que demonstra coerência metodológica. A implementação de procedimento formal de consolidação periódica entre os dois instrumentos fortaleceria ainda mais essa integração.

Oportunidade 5 - Autorização: o NIST RMF prevê que autoridade formalmente designada documente a decisão de aceitar o risco residual, com prazo de validade, procedimento que não foi identificado nos documentos analisados. Sua implementação fortaleceria a rastreabilidade decisória, convergindo com o princípio da LAI: decisões sobre gestão de riscos registradas e assinadas por autoridade competente tornam-se facilmente acessíveis em eventual pedido de informação, demonstrando transparência e responsabilização. A Adaptação 5 propõe a estruturação desse processo.

4.4 Risco emergente: Inteligência Artificial e ABNT NBR 23894:2023

A organização não utiliza sistemas de Inteligência Artificial em sua infraestrutura institucional. A rede EBNet, gerenciada pelo CITEEx, restringe o acesso a ferramentas de IA nos equipamentos institucionais, controle de acesso válido, mas não equivalente a um processo de gestão de riscos de IA.

Três razões justificam a inclusão do tema mesmo sem uso atual. Primeiro: risco de uso informal em dispositivos pessoais, não tratado nas normas vigentes. Segundo: o DECEEx já utiliza IA no EBAula e a Diretriz EB20-D02.031 sinaliza trajetória institucional de adoção. Terceiro: a ABNT NBR 23894:2023 orienta que organizações sem uso atual de IA devem avaliar riscos de adoção futura e incluir essa categoria no processo de gestão de riscos.

Recomenda-se que os planos de gestão de risco em organizações deste perfil contemplem essa dimensão de antecipação.

4.5 Conformidade com LAI e LGPD: avaliação específica

A análise específica da aderência à LAI e à LGPD revela um padrão positivo: a organização já pratica controles de fato, restringe o acesso a sistemas, classifica documentos conforme as IGSAS, limita o uso de equipamentos institucionais. A oportunidade identificada é a formalização desses controles em instrumentos normativos que respondam também às exigências legais de transparência (LAI) e proteção de dados (LGPD). O Quadro abaixo sintetiza a avaliação.

Em relação à LAI, três oportunidades de aprimoramento foram identificadas. (1) a estruturação de página de transparência ativa nos termos do art. 8º da LAI e do Decreto nº 7.724/2012, com publicação proativa de estrutura organizacional, competências, dados orçamentários e respostas a perguntas frequentes; (2) a implementação de revisão periódica das classificações de sigilo, conforme recomendado pelo art. 35 da lei, garantindo a atualidade das marcações; e (3) o registro formal das decisões de gestão de riscos em formato rastreável, instrumentalizando a transparência decisória.

Em relação à LGPD, cinco oportunidades de estruturação formal foram identificadas nos documentos analisados: (1) elaboração de mapeamento de fluxo de dados pessoais (data mapping), que consolida em um único instrumento todas as categorias de dados tratadas, suas bases legais e medidas de proteção; (2) indicação formal de Encarregado pelo Tratamento de Dados Pessoais (DPO), conforme art. 41 da LGPD, função acumulável por servidor já existente; (3) elaboração de Relatório de Impacto à Proteção de Dados (RIPD) para o tratamento de dados de menores, recomendado pelo art. 38 e pela Resolução ANPD nº 2/2022; (4) estruturação de procedimento de resposta a incidentes com dados pessoais, incluindo protocolo de comunicação à ANPD (art. 48) e aos titulares; e (5) registro explícito da base legal aplicável a cada categoria de dado tratado, documentação que evidencia a conformidade já existente na prática. Esses cinco pontos compõem a Oportunidade 6.

Oportunidade 6 - LGPD e LAI: estruturação da conformidade jurídica formal. A organização já realiza controles de proteção de dados e de sigilo na prática; a oportunidade

consiste em formalizar esses controles por meio de data mapping, indicação de DPO, elaboração de RIPD para dados de menores e estruturação de procedimento de notificação de incidentes. No âmbito da LAI, a implementação de transparência ativa estruturada e de revisão periódica das classificações de sigilo completa o alinhamento jurídico. Essas ações, em conjunto, consolidam formalmente práticas que a organização já demonstra no cotidiano.

5 PROPOSTAS DE ADAPTAÇÕES

As sete adaptações propostas decorrem diretamente das oportunidades de aprimoramento identificadas, incluindo a Oportunidade 6 (conformidade jurídica LGPD/LAI). Todas partem do arcabouço normativo atual, sem exigir reconstrução, trata-se de formalizar e integrar práticas que a organização já realiza. As três primeiras estão sob controle da própria organização; as quatro últimas envolvem articulação com outras áreas ou com o escalão superior.

Nº	Adaptação	Norma	Responsável	Prazo
1	Integração formal PSI/CGSI ↔ Plano de Gestão de Riscos	ISO 31000, cl. 5.3	EGP	Até 6 meses
2	Campo de risco residual nos formulários e reunião semestral de retroalimentação	ISO 31000, cl. 5.6–5.7; NIST Monitoramento	Comitê de Governança	Até 6 meses
3	Ampliação do Anexo A com partes interessadas e ameaças do ambiente de ensino	ISO 31000, cl. 6.3; NIST Preparação	EGP	Próxima revisão anual
4	Consolidação semestral plano TI ↔ Plano de Gestão de Riscos	ISO 31000, cl. 5.3; NIST Categorização	Ch Sec Infor e EGP	6 a 12 meses
5	Processo formal de autorização com autoridade designada e prazo de validade	NIST Autorização; ISO 31000, cl. 6.5.3	Subcomandante e Gerência SI	6 a 12 meses

Nº	Adaptação	Norma	Responsável	Prazo
6	Categoria de risco de IA no Plano, com registro da restrição EBNet e revisão anual	ABNT NBR 23894:2023; EB20-D02.031	EGP e CGSI	6 a 12 meses
7	Estruturação da conformidade LGPD e LAI: data mapping, DPO, RIPD, protocolo ANPD e transparência ativa	LGPD, arts. 14, 37, 41, 48; LAI, art. 8º; Decreto nº 7.724/2012	Sec Pessoal + CGSI + assessoria jurídica do escalão superior	Até 6 meses

Tabela 2. Resumo das sete adaptações propostas.

Adaptação 1 - Integração formal entre PSI/CGSI e o Plano de Gestão de Riscos: recomenda-se a criação de procedimento formal de articulação entre o CGSI, vinculado à PSI e alinhado à ISO 27001, e o EGP, gestor do Plano de Gestão de Riscos alinhado à ISO 31000:2018. O procedimento deve definir: critérios de relevância para encaminhamento recíproco de ocorrências e deliberações; periodicidade mínima de reunião conjunta semestral; e formato padronizado de registro das decisões. Trata-se de formalizar a articulação que já ocorre entre os dois instrumentos, conferindo rastreabilidade e continuidade.

Adaptação 2 - Retroalimentação documentada das auditorias ao Plano de Gestão de Riscos: recomenda-se a inclusão de campo padronizado de "risco residual identificado" nos formulários de auditoria de TI, com encaminhamento ao EGP ao término de cada ciclo. Reunião semestral formal de retroalimentação fecha o ciclo de melhoria contínua previsto na cláusula 5.7 da ISO 31000:2018 e na etapa de Monitoramento do NIST RMF, fortalecendo a coerência entre auditoria e gestão de riscos.

Adaptação 3 - Ampliação do contexto organizacional para o perfil de ensino: recomenda-se ampliar o Anexo A da PSI para contemplar as partes interessadas do ambiente de ensino: alunos e responsáveis legais, parceiros acadêmicos e prestadores de serviço educacional. A Matriz de Riscos pode ser enriquecida com ameaças próprias desse perfil: acesso indevido a registros acadêmicos, uso de dispositivos pessoais por alunos, compartilhamento de dados de menores e incidentes com parceiros externos. Essa ampliação é também condição prévia para o data mapping e o RIPD da Adaptação 7.

Adaptação 4 - Consolidação periódica entre o Plano Diretor de TI e o Plano de Gestão de Riscos: recomenda-se instituir procedimento semestral de consolidação entre os dois instrumentos, com reunião conjunta entre o Chefe da Seção de Informações e o EGP, ata de registro de divergências e atualização coordenada dos planos. A coerência metodológica já existente entre os documentos, elaborados pela mesma equipe, facilita a implementação: trata-se de estruturar formalmente o que já ocorre.

Adaptação 5 - Processo formal de autorização e registro de risco residual: recomenda-se instituir formulário pelo qual a autoridade competente, Subcomandante ou Gerente de SI formalmente designado, documenta a decisão de aceitar determinado risco residual, com: fundamentação técnica, referência à Matriz de Riscos, data, prazo de validade e assinatura. O documento integra o arquivo de gestão de riscos e serve de resposta a eventuais solicitações de acesso à informação via LAI, demonstrando transparência e responsabilização.

Adaptação 6 - Inclusão de categoria de risco de Inteligência Artificial no Plano de Gestão de Riscos: recomenda-se criar categoria de risco de IA na Matriz de Riscos, contemplando o uso informal de ferramentas de IA generativa em dispositivos pessoais de alunos e servidores, não coberto pelos controles da EBNet; a perspectiva de adoção institucional de sistemas de IA, em linha com a Diretriz EB20-D02.031 e a experiência do DECEX com o EBAula; e os riscos à privacidade e ao sigilo decorrentes de modelos que processam dados institucionais. Recomenda-se ainda registrar formalmente a restrição EBNet como controle implementado e programar revisão anual da categoria.

Adaptação 7 - Estruturação da conformidade LGPD e LAI: esta adaptação desdobra-se em cinco ações sequenciais: elaborar mapeamento de fluxo de dados pessoais (data mapping) cobrindo todas as categorias de dados tratadas pela organização, com identificação de bases legais, finalidades, prazos de retenção e medidas de proteção aplicadas; indicar formalmente o Encarregado pelo Tratamento de Dados Pessoais (DPO), conforme art. 41 da LGPD, função acumulável por servidor já existente, mediante designação formal; elaborar o Relatório de Impacto à Proteção de Dados (RIPD) para o tratamento de dados de alunos menores, contemplando os riscos identificados e os controles mitigadores já em vigor; estruturar procedimento de resposta a incidentes com dados pessoais, incluindo protocolo de comunicação à ANPD (art. 48 LGPD) e aos titulares; e implementar página de transparência ativa conforme Decreto nº 7.724/2012. A integração desta adaptação com a Adaptação 5

(registro formal de aceitação de risco residual) é recomendada: o documento de autorização de risco residual serve simultaneamente como instrumento de rastreabilidade para fins da LAI e como registro de responsabilização para fins da LGPD.

6 CONCLUSÃO

O resultado deste trabalho confirmou que a Organização Militar de Ensino analisada dispõe de estrutura sólida e madura de gestão de riscos em segurança da informação. Possui Política de Segurança da Informação aprovada em 2026, alinhada à ISO 27001, com CGSI formalmente constituído; Plano de Gestão de Riscos que cita explicitamente a ISO 31000:2018; Matriz de Riscos com avaliação de probabilidade e impacto; e Plano de Auditoria de TI estruturado, conjunto normativo que supera o que as IGSAS isoladas sugerem. A análise identificou ainda oportunidades de alinhamento formal com a LGPD e a LAI, cujos instrumentos, data mapping, DPO, RIPD e transparência ativa, complementariam o arcabouço já existente.

O que o gap analysis revelou foi a oportunidade de avançar na integração e na formalização, técnica e jurídica. PSI e CGSI, alinhados à ISO 27001, e o Plano de Gestão de Riscos, alinhado à ISO 31000:2018, coexistem com oportunidade de articulação formal. As auditorias podem retroalimentar o plano de forma mais documentada. O Plano Diretor de TI pode ser periodicamente consolidado com o plano institucional. O processo de autorização formal para aceitação de risco residual, previsto no NIST RMF e instrumentalmente útil para a rastreabilidade da LAI, pode ser estruturado. E os instrumentos da LGPD, data mapping, DPO, RIPD e protocolo de resposta a incidentes, podem ser formalmente implementados, consolidando práticas que a organização já realiza.

A Oportunidade 5, formalização do processo de autorização, é a que mais diretamente responde à pergunta central deste trabalho quanto à dimensão técnica, pois registrar formalmente quem decide sobre controles de segurança, com qual fundamentação e qual risco residual aceito, confere rastreabilidade e fortalece a governança. A Oportunidade 6, estruturação da conformidade com LGPD e LAI, complementa essa dimensão com o alinhamento jurídico necessário para uma organização que trata dados de menores e está sujeita a obrigações de transparência. As Adaptações 5 e 7 endereçam, em conjunto, essas oportunidades.

A incorporação da ABNT NBR 23894:2023, sugerida pelo professor orientador, revelou dimensão adicional de interesse. O Exército já possui política institucional sobre IA (Diretriz EB20-D02.031) e o DECEX já a utiliza no EBAula, demonstração de trajetória institucional consistente. A restrição via EBNet é controle de acesso válido; sua complementação com processo de gestão de riscos de IA representa o passo seguinte natural. A interface com a LGPD é direta: sistemas de IA que processem dados de alunos menores demandarão RIPD específico e documentação de base legal.

Verifica-se que todos os objetivos do trabalho foram atendidos. O arcabouço normativo foi mapeado; o gap analysis foi conduzido em relação à ISO 31000:2018, ao NIST RMF e à ABNT NBR 23894:2023; a aderência à LGPD e à LAI foi avaliada; e sete adaptações foram propostas com responsáveis e prazos. Todas partem do que existe, nenhuma exige reconstrução. A convergência entre as exigências do NIST RMF (registro formal de aceitação de risco residual) e da LAI (rastreadabilidade decisória) é a principal contribuição conceitual deste trabalho: demonstra que conformidade técnica e conformidade jurídica, frequentemente tratadas como trilhas separadas, convergem no mesmo instrumento, o documento de autorização de risco residual. Para pesquisas futuras, estudos comparativos entre instituições militares de ensino e instituições de civis, quanto à implementação da LGPD, e avaliações pós-implementação das adaptações propostas, seriam contribuições relevantes para o campo.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR 16337:2020 - Gestão de riscos: diretrizes. Rio de Janeiro: ABNT, 2020.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR 23894:2023 - Tecnologia da informação - Inteligência artificial - Orientação sobre gestão de riscos. Rio de Janeiro: ABNT, 2023.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. 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, Brasília, 28 jan. 2022.

BRASIL. Decreto nº 79.099, de 6 de janeiro de 1977. Aprova o Regulamento para Salvaguarda de Assuntos Sigilosos. Diário Oficial da União, Brasília, 7 jan. 1977.

BRASIL. Lei nº 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal. Diário Oficial da União, Brasília, 18 nov. 2011.

BRASIL. Decreto nº 7.724, de 16 de maio de 2012. Regulamenta a Lei nº 12.527/2011, que dispõe sobre o acesso a informações previsto na Constituição Federal. Diário Oficial da União, Brasília, 16 mai. 2012.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Brasília, 15 ago. 2018.

BRASIL. Ministério da Defesa. Exército Brasileiro. Portaria nº 1.067-Cmt Ex, de 8 de setembro de 2014. Aprova as IGSAS (EB10-IG-01.011). Separata ao Boletim do Exército nº 37/2014.

BRASIL. Ministério da Defesa. Exército Brasileiro. Portaria nº 225-EME, de 26 de julho de 2019. Aprova a Diretriz Reguladora da Política de Gestão de Riscos do Exército Brasileiro (EB20-D-02.010).

BRASIL. Ministério da Defesa. Exército Brasileiro. Portaria nº 292-EME, de 2 de outubro de 2019. Aprova o Manual Técnico de Gestão de Riscos do Exército Brasileiro (EB20-MT-02.001).

BRASIL. Ministério da Defesa. Exército Brasileiro. Portaria EME/C Ex nº 1.318, de 14 de maio de 2024. Aprova a Diretriz Estratégica de Inteligência Artificial (EB20-D02.031).

CALDER, Alan; WATKINS, Steve. IT Governance: An International Guide to Data Security and ISO 27001/ISO 27002. 7. ed. Londres: Kogan Page, 2019.

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

LIMA, Rogério et al. Avaliação da maturidade em segurança da informação em organizações públicas brasileiras: um estudo comparativo entre o framework CIS CSC e as normas do ONS. Revista Brasileira de Segurança da Informação, v. 4, n. 1, p. 45–67, 2022.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. ISO 31000:2018, Risk management: Guidelines. 2. ed. Genebra: ISO, 2018.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. NIST Special Publication 800-37, Revision 2: Risk Management Framework for Information Systems

and Organizations. Gaithersburg: NIST, 2018. Disponível em:
<https://doi.org/10.6028/NIST.SP.800-37r2>. Acesso em: jul. 2026.

TRIBUNAL DE CONTAS DA UNIÃO. Referencial básico de gestão de riscos. Brasília: TCU, 2018.