POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

PSI

DIRETOR PRESIDENTE

Marcelo Azeredo Cornélio

ELABORAÇÃO DO DOCUMENTO

Assessoria de Segurança da Informação e de Gestão de Riscos - ASSIG

Sumário

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO – PSI

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	
Área Responsável:	ASSIG - Assessoria de Segurança da Informação e Gestão de Riscos
Aprovado por:	Diretoria Geral – DIGER Diretoria Setorial Técnica – DSTEC
Data da Aprovação	Instrução de Serviço nº 009-N, Publicada em 22 de junho de 2026.
Data da Última Revisão	21/05/2026
Versão	2.0
Classificação	Público

1. Objetivo

Esta Política visa definir responsabilidades, deveres e penalidades quanto à segurança da informação, além de promover uma cultura de proteção às informações — sejam elas do PRODEST, do governo, do cidadão, de outros órgãos ou entidades, dos fornecedores, bem como de outras partes envolvidas em acordos com o Instituto.

2. Abrangência

2.1. Esta Política aplica-se aos servidores, estagiários, fornecedores, prestadores de serviços contratados direta ou indiretamente (terceirizados), outras partes interessadas e aos envolvidos em acordos com o PRODEST (independentemente dos instrumentos administrativos utilizados para tal). Isso inclui pessoas que trabalhem em período integral, meio período ou em regime temporário, seja em atuação presencial ou remota.

2.2. **Parágrafo único**. Servidores, fornecedores, prestadores de serviço, estagiários e demais profissionais que atuem pelo PRODEST podem ser referidos nesta Política simplesmente como “colaboradores”.

3. Termos e definições

Para os efeitos desta Política, consulte o documento Glossário de Segurança da Informação, aprovado pela Portaria GSI/PR Nº 93, de 18 de outubro de 2021.

4. Papéis e Responsabilidades

4.1. A Alta Direção é responsável por assegurar o comprometimento institucional com a segurança da informação, provendo recursos, apoio e direcionamento para a implementação e manutenção das diretrizes estabelecidas nesta Política. É de sua responsabilidade aprovar esta Política, zelar por sua efetividade e garantir que a segurança da informação seja tratada como parte integrante da gestão organizacional.

4.2. Compete a Assessoria de Segurança da Informação e de Gestão de Riscos (ASSIG) coordenar e supervisionar as ações relativas à proteção das informações do PRODEST. Cabe-lhe propor melhorias, avaliar riscos, promover a conformidade com esta Política e normas aplicáveis, além de orientar usuários e gestores na adoção de práticas seguras com relação à segurança da informação.

4.3. Compete ao Gestor de Riscos e Continuidade (representante da ASSIG) estabelecer, manter e operacionalizar os processos de gestão de riscos e de continuidade de negócios, consolidando e analisando os resultados produzidos pelas áreas operacionais, mantendo atualizada a matriz de riscos e seus respectivos planos de tratamento, bem como verificando e acompanhando a elaboração e os testes dos planos de continuidade e recuperação de desastres em conjunto com as unidades organizacionais envolvidas.

4.4. Compete ao Gestor de Segurança Cibernética (representante da ASSIG) apoiar a Alta Direção nas ações relacionadas à segurança cibernética, integrar os processos de segurança aos demais processos organizacionais, coordenar a gestão de incidentes consolidando informações relevantes para os processos de segurança e de riscos, garantir a comunicação entre os gestores operacionais e a Alta Direção, apoiar iniciativas de conscientização e coordenar, em conjunto com as áreas operacionais, as ações decorrentes do monitoramento realizado pelo SOC.

4.5. Gestores Operacionais de Segurança Cibernética (representantes das Gerências de Plataforma de TIC, Sistemas, Dados e Integração) são responsáveis por implementar e manter controles técnicos e administrativos pertinentes às suas áreas, realizar atividades de monitoramento, resposta e recuperação, identificar e classificar ativos e vulnerabilidades, elaborar planos de recuperação de desastres alinhados às necessidades do negócio, avaliar riscos e contramedidas, bem como interagir com o SOC nas atividades de resposta a incidentes.

4.6. Compete ao Encarregado Interno pelo Tratamento de Dados Pessoais (DPO) atuar como ponto de contato institucional em assuntos relacionados à proteção de dados pessoais, nos termos do Artigo 41 da LGPD, na Resolução CD/ANPD No 18 e da Política Estadual de Proteção de Dados Pessoais e da Privacidade do Poder Executivo Estadual - Decreto Estadual nº 4.922-R, de 09 de julho de 2021.

4.7. Gerentes e representantes de todas as unidades organizacionais devem assegurar que suas equipes conheçam, compreendam e cumpram as diretrizes desta Política. Devem zelar pelo uso adequado dos recursos sob sua responsabilidade e colaborar com o processo de identificação e tratamento de riscos ou incidentes que envolvam suas unidades.

4.8. Colaboradores, usuários e demais partes interessadas são responsáveis por adotar conduta ética e segura no uso das informações e recursos institucionais, respeitando as orientações desta Política e reportando imediatamente qualquer evento que possa representar ameaça à segurança da informação.

4.9. O PRODEST deverá instituir um Comitê de Segurança da Informação e Gestão de Riscos, de natureza executiva, consultiva e deliberativa, responsável por estabelecer diretrizes, aprovar políticas e controles, definir o apetite e a tolerância a riscos e deliberar sobre sua priorização e aceitação, solicitar indicadores e monitorar a efetividade dos controles, avaliar respostas a incidentes, e promover a conformidade com requisitos legais, regulatórios e normativos aplicáveis, nos termos do seu ato de instituição.

4.10. Como órgão responsável pela Tecnologia da Informação e Comunicação (TIC) do Governo do Estado do Espírito Santo, o PRODEST compartilha as obrigações de segurança da informação e privacidade com os órgãos clientes, variando o nível de responsabilidade técnica conforme modelo de serviço contratado.

4.11. Compete ao PRODEST assegurar a disponibilidade, a segurança e a operação da infraestrutura e dos serviços ofertados, enquanto os órgãos clientes permanecem responsáveis pela gestão, qualidade, uso e conformidade dos dados sob sua titularidade ou responsabilidade, conforme aplicável.

5. Diretrizes

As diretrizes estabelecidas nesta Política (para criação, transmissão, processamento, utilização, armazenamento, recuperação e descarte de informações) são norteadas pelos princípios de:

I - **confidencialidade:** garantia de que a informação está acessível somente para pessoas, entidades ou processos autorizados;

II - **integridade:** garantia de que a informação está íntegra, exata;

III - **disponibilidade:** garantia de que a informação pode ser acessada pelas pessoas, entidades ou processos autorizados, quando for necessário;

IV - **autenticidade:** garantia de que a origem da informação é verificável e a entidade é o que alega ser;

V - **legalidade:** garantia de que o tratamento da informação ocorre de acordo com as legislações vigentes;

VI - **finalidade:** o tratamento é realizado para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

6. Declarações da política

Seção I - Propriedade intelectual

Art. 1. Toda informação produzida nos ambientes internos, como resultado de atividades contratadas pelo Instituto, pertence ao PRODEST ou aos seus respectivos proprietários beneficiários, devendo as exceções serem explicitamente formalizadas.

Art. 2. O PRODEST proíbe a instalação, utilização ou distribuição de softwares que não possuam a devida licença ou autorização para uso, respeitando os contratos firmados e as legislações vigentes, em consonância com o disposto na Instrução de Serviço nº 069-N, de 30 de novembro de 2020, que trata do combate à pirataria de software e a demais crimes que infrinjam direitos autorais.

Seção II - Confidencialidade ou não divulgação

Art. 3. Colaboradores, usuários e partes interessadas devem estar cientes do seu compromisso com a confidencialidade das informações do PRODEST, bem como aquelas de terceiros tratadas sob a sua responsabilidade.

Art. 4. O PRODEST estabelece um Termo de Compromisso padronizado para conhecimento e assinatura de colaboradores, usuários e outras partes interessadas para tratar o tema da confidencialidade ou não divulgação.

Seção III - Gestão de riscos de segurança da informação

Art. 5. Diretrizes, estratégias e processos formalizados para a gestão de riscos de segurança da informação devem ser definidos, implementados e mantidos com base em boas práticas e *frameworks* reconhecidos de mercado e normas nacionais e internacionais aplicáveis.

Parágrafo único. Os riscos devem ser identificados, registrados, atribuídos a um proprietário, avaliados quanto à probabilidade e ao impacto, monitorados e tratados, de acordo com os critérios padronizados estabelecidos pelo PRODEST.

Seção IV - Tratamento da informação

Art. 6. O PRODEST deve assegurar, no limite de suas atribuições, que as informações sob sua responsabilidade, independentemente do suporte, formato ou meio de transmissão, sejam tratadas de forma a garantir sua confidencialidade, integridade e disponibilidade, ao longo de todo o seu ciclo de vida.

§ 1º O uso, o armazenamento e a transferência de informações devem observar rigorosamente seu nível de sigilo, limitando o acesso estritamente a pessoas autorizadas e para finalidades institucionais legítimas.

§ 2º As diretrizes de tratamento devem estar alinhadas com boas práticas e *frameworks* reconhecidos de mercado, bem como normas nacionais e internacionais aplicáveis.

Art. 7. O descarte de informações e a desativação de ativos que as contenham devem ser realizados por meio de métodos seguros que impeçam a recuperação não autorizada dos dados.

§ 1º Dispositivos e mídias destinados ao descarte ou reutilização devem passar por processos de sanitização (expurgo) validados, conforme as melhores práticas de segurança e normas ambientais vigentes.

§ 2º A exclusão de dados em sistemas complexos ou mídias de backup deve considerar a viabilidade técnica e as obrigações legais de retenção (*Legal Hold*), sem prejuízo à segurança da informação.

Art. 8. A implementação dos controles de tratamento de informação deve ser periodicamente revisada para assegurar a conformidade com as evoluções tecnológicas e as exigências da LGPD (Lei Geral de Proteção de Dados), priorizando sempre a adoção de padrões internacionais de excelência em governança e risco.

Seção V - Gestão de acesso lógico

Art. 9. O acesso lógico a sistemas e ativos de informação do PRODEST deve ser concedido de forma controlada, limitada aos usuários autorizados e aos privilégios necessários para o desempenho de suas funções, atendendo aos princípios do privilégio mínimo *(least privilege*) e necessidade de saber (*need-to-know*).

Art. 10. O ciclo de vida do acesso (concessão, revisão periódica, alteração e revogação imediata no desligamento) deve ser formalizado e auditável, devendo a governança de acessos observar *frameworks* de identidade como NIST SP 800-63 e as recomendações da ISO/IEC 27001:2022 e ISO/IEC 27002:2022.

Art. 11. Devem ser adotados mecanismos robustos de autenticação para proteger a identidade digital dos colaboradores e a integridade dos sistemas, priorizando-se o uso de Autenticação de Múltiplos Fatores (MFA) em todos os serviços críticos e acessos remotos.

Art. 12. Os usuários devem seguir a Instrução Normativa nº 005/2025-N de 07 de agosto de 2025 (“Política Padrão de Autenticação” do PRODEST), para demais diretrizes sobre gestão de acessos e autenticação.

Seção VI - Segurança física e de ambiente

Art. 13. O PRODEST deve adotar medidas de segurança física que protejam seus ativos de informação, instalações, equipamentos e pessoas contra acesso não autorizado, danos, furtos ou qualquer ameaça que possa comprometer a segurança das informações. Tais medidas devem ser revisadas periodicamente, incorporando melhorias contínuas e ajustes de controles conforme mudanças nas instalações, operações ou riscos identificados.

Art. 14. O acesso às instalações e áreas críticas deve ser controlado e restrito a pessoas autorizadas, garantindo que procedimentos de entrada, circulação e saída estejam de acordo com as diretrizes de segurança da informação. Equipamentos, mídias e dispositivos que contenham informações institucionais devem ser armazenados de forma segura, protegidos contra danos físicos, roubo, perda ou acesso indevido.

Art. 15. A infraestrutura predial e os ambientes tecnológicos do PRODEST devem ser projetados e mantidos para assegurar a disponibilidade e a integridade dos ativos de informação.

Art. 16. O ciclo de vida físico dos ativos, incluindo instalação, manutenção e remoção das dependências, deve ser formalmente gerenciado para evitar a perda ou exposição indevida de informações.

Art. 17. A segurança física e de ambiente deve observar padrões reconhecidos, como a ANSI/TIA-942 (requisitos para data centers), ISO/IEC 27001:2022 e NIST Cybersecurity Framework (CSF).

Seção VII - Uso responsável de Inteligência Artificial (IA)

Art. 18. O desenvolvimento, a implementação, o uso e o monitoramento de sistemas, serviços, ferramentas e recursos de Inteligência Artificial (IA) devem observar as melhores práticas e *frameworks* reconhecidos de mercado, como a ISO/IEC 42001:2023 (sistema de gestão de IA), o NIST AI RMF (gerenciamento de riscos associados à IA) e o ITIL v5 (gerenciamento de serviços e produtos digitais), considerando os objetivos institucionais, a gestão de riscos, a criticidade das operações e a classificação das informações tratadas.

Art. 19. O uso de recursos de IA no âmbito do PRODEST deve observar, cumulativamente, os princípios da rastreabilidade, supervisão humana efetiva e responsabilização pelos resultados.

Seção VIII - Desenvolvimento de software interno ou terceirizado

Art. 20. Todos os sistemas, aplicações e softwares desenvolvidos ou adquiridos pelo PRODEST devem considerar princípios de segurança da informação e privacidade desde a concepção até a operação, visando proteger as informações no âmbito do Instituto.

Art. 21. O planejamento e implementação de medidas de segurança devem estar previstos ao longo de todo o ciclo de vida de desenvolvimento conforme melhores práticas e *frameworks* reconhecidos de mercado, como o Microsoft SDL – Security Development Lifecycle.

Art. 22. Desenvolvedores, fornecedores e terceiros envolvidos no desenvolvimento ou na manutenção de sistemas devem estar cientes de suas responsabilidades quanto à segurança da informação e aderir às diretrizes institucionais. Alterações, atualizações ou correções de sistemas devem ser gerenciadas de forma controlada e auditável, assegurando que mudanças não comprometam a segurança ou a operação dos ativos de informação.

Seção IX - Gestão de fornecedores

Art. 23. O PRODEST deve assegurar que todos os fornecedores, prestadores de serviço e parceiros que tenham acesso a ativos de informação ou realizem atividades críticas estejam alinhados à esta Política e documentos complementares aplicáveis, implementando medidas compatíveis com os requisitos do Instituto e preservando a confidencialidade, a integridade e a disponibilidade das informações.

Art. 24. Fornecedores identificados como operadores de dados pessoais, nos casos em que o PRODEST atuar como controlador, devem demonstrar conformidade com a LGPD e demais regulamentos aplicáveis.

Art. 25. É responsabilidade do PRODEST avaliar e gerenciar os riscos relacionados aos fornecedores, definindo de forma clara nos contratos as obrigações de segurança, responsabilidades e mecanismos de monitoramento.

Art. 26. Todas as partes envolvidas em contratos ou editais do PRODEST devem tratar todas as informações que receberem ou tiverem acesso com sigilo e responsabilidade, devendo manter todas as boas práticas reconhecidas de mercado em segurança da informação e privacidade.

Seção X - Incidentes de segurança da informação e privacidade

Art. 27. O PRODEST deve estabelecer uma estratégia formal para gestão de incidentes de segurança da informação e privacidade, observando as melhores práticas e *frameworks* reconhecidos de mercado, como a ISO/IEC 27035 e o NIST SP 800-61, assegurando que ações apropriadas sejam adotadas para minimizar impactos sobre os ativos, processos e informações do Instituto.

Art. 28. Plano(s) de resposta a incidentes devem ser desenvolvidos, mantidos e testados periodicamente, assegurando que os procedimentos de resposta sejam eficazes e adequados à criticidade dos processos, sistemas e ativos do PRODEST.

Art. 29. Todos os usuários devem comunicar quaisquer incidentes de segurança da informação ocorridos ou prováveis de ocorrerem (eventos), através das ferramentas disponibilizadas pelo Instituto.

§ 1º Quando possível, deve-se anexar provas ou evidências do fato, desde que sua produção não descaracterize o cenário afetado ou infrinja a Política de Segurança da Informação do PRODEST ou qualquer legislação em vigor.

Seção XI - Continuidade de negócios e recuperação de desastres

Art. 30. O PRODEST deve definir e manter diretrizes, estratégias e processos formalizados para assegurar a continuidade dos negócios e a recuperação em caso de desastres, assegurando alinhamento aos objetivos institucionais, às melhores práticas e *frameworks* reconhecidos pelo mercado, como a ISO/IEC 22301:2019 (sistemas de gestão de continuidade de negócios), ISO/IEC 27031:2025 (prontidão de TIC para continuidade de negócios) e ITIL v5 (gerenciamento de serviços e produtos digitais).

Art. 31. Planos de continuidade de negócios e planos de recuperação de desastres devem ser desenvolvidos, mantidos e testados periodicamente, assegurando que os procedimentos de recuperação sejam eficazes e adequados à criticidade dos processos e sistemas envolvidos.

Art. 32. O PRODEST deve assegurar que os ativos tecnológicos disponham de redundância adequada, bem como de controles de segurança da informação e privacidade implementados, de forma a assegurar o cumprimento dos requisitos de disponibilidade da informação e objetivos definidos para resposta a incidentes, continuidade de negócios e recuperação de desastres.

Seção XII - Documentos Complementares

Art. 33. Convém que esta Política seja apoiada por políticas, normas, procedimentos e demais documentos específicos por tema, sempre que necessário, com a finalidade de estabelecer, detalhar e reforçar a implementação de controles de segurança da informação, assegurando a cobertura adequada dos diferentes domínios e áreas de segurança no âmbito do PRODEST.

§ 1º Áreas que executem atividades ou processos em atendimento a esta Política, ou que realizem outros procedimentos direta ou indiretamente relacionados à segurança da informação ou à gestão de riscos, devem elaborar e manter atualizados documentos próprios que os normatizem.

Seção XIII - EXCEÇÕES

Art. 34. Qualquer situação que não se enquadre nas diretrizes desta Política deve ser formalmente identificada como exceção e submetida à área responsável pela avaliação de medidas compensatórias e homologada pelo Comitê de Segurança da Informação e Gestão de Riscos ou pela Alta Direção.

Seção XIV - PROCESSO DISCIPLINAR

Art. 35. O descumprimento desta Política poderá ensejar medidas administrativas, disciplinares e/ou contratuais cabíveis, mediante apuração formal, observada a legislação aplicável e o regime jurídico pertinente ao vínculo do agente (servidor, estagiário, empregado, terceirizado ou fornecedor), sem prejuízo de responsabilização civil e penal quando aplicável.

Seção XV- REVISÃO

Art. 36. Esta Política entrará em vigor na data de sua publicação e deverá ser revisada anualmente, ou extraordinariamente, sempre que necessário.

Seção XVI – REFERÊNCIAS LEGAIS E NORMATIVAS

Art. 37. Esta Política foi estabelecida considerando as seguintes referências normativas e legais:

I - Leis Federais e Estaduais:

a. Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação);

b. Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet);

c. Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais);

d. Lei nº 14.129, de 29 de março de 2021 (Lei do Governo Digital);

e. Lei Estadual nº 9.871, de 09 de julho de 2012, que dispõe sobre normas de acesso à informação no Estado do Espírito Santo;

f. Lei Complementar nº 1.064, de 19 de dezembro de 2023, que reorganiza a estrutura organizacional básica do PRODEST.

II - Decretos e Regulamentações:

a. Decreto nº 2.884-R, de 21 de outubro de 2011, que instituiu a Política Estadual de Segurança da Informação (PESI);

b. Decreto nº 3.152-R, de 26 de novembro de 2012, que regulamenta a Lei Estadual nº 9.871/2012;

c. Decreto nº 4.505-R, de 20 de setembro de 2019, que instituiu a Política Estadual de Tecnologia da Informação e Comunicação (PETI);

d. Decreto nº 4.922-R, de 09 de julho de 2021, que institui a Política Estadual de Proteção de Dados Pessoais e da Privacidade (PEPDP), alterado pelo Decreto nº 5.198-R, de 18 de agosto de 2022;

e. Decreto nº 6.095-R, de 08 de julho de 2025, que regulamenta a prestação dos serviços do PRODEST.

III - Normativos Internos do PRODEST:

a. Política de Privacidade do PRODEST, disponível em https://prodest.es.gov.br/privacidade;

b. Instrução de Serviço nº 076, de 14 de outubro de 2021, substituída pela Instrução de Serviço nº 034-P, de 29 de julho de 2025, que designa o Encarregado pelo Tratamento de Dados Pessoais titular e substituto do PRODEST.

IV - Normas e *frameworks* técnicos:

a. ABNT NBR ISO/IEC 27001:2022 – Segurança da informação, segurança cibernética e proteção à privacidade — Sistemas de gestão da segurança da informação — Requisitos;

b. ABNT NBR ISO/IEC 27002:2022 – Segurança da informação, segurança cibernética e proteção à privacidade — Controles de segurança da informação;

c. ABNT NBR ISO/IEC 27701:2019 – 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;

d. NIST Cybersecurity Framework (CSF) 2.0;

e. CIS Critical Security Controls Version 8.1.

MARCELO AZEREDO CORNELIO

Diretor Geral/Presidente – PRODEST

SANDRO JOSÉ CARVALHO ALVES

Diretor Setorial Técnico – PRODEST

Documento original assinado eletronicamente, conforme MP 2200-2/2001, art. 10, § 2º, por:

MARCELO AZEREDO CORNÉLIO
DIRETOR GERAL
PRODEST - PRODEST - GOVES
assinado em 19/06/2026 14:58:44 -03:00

SANDRO JOSE CARVALHO ALVES
DIRETOR SETORIAL
DSTEC - PRODEST - GOVES
assinado em 19/06/2026 14:47:18 -03:00

INFORMAÇÕES DO DOCUMENTO
Documento capturado em 19/06/2026 14:58:44 (HORÁRIO DE BRASÍLIA - UTC-3)
por ELISANGELA FERRARI DE MELLO (FG GESTOR DE PROGRAMAS E PROJETOS - UECI - PRODEST - GOVES)
Valor Legal: ORIGINAL | Natureza: DOCUMENTO NATO-DIGITAL

A disponibilidade do documento pode ser conferida pelo link: https://e-docs.es.gov.br/d/2026-JPJFNK