PUC
RIO

# Política de Segurança da Informação

voar mais alto

PUC
RIO

**Reitor**
Pe. Anderson Antonio Pedroso, S.J.

**Vice-Reitor**
Pe. Miguel Martins de Oliveira Filho, S.J.

**Vice-Reitora Acadêmica (Ensino e Pesquisa)**
Profa. Marley Vellasco

**Vice-Reitor Administrativo**
Prof. Leonardo Lima

**Vice-Reitor Comunitário**
Prof. Renato Callado

**Vice-Reitor de Desenvolvimento e Inovação**
Prof. Marcelo Gattass

**Vice-Reitora de Extensão e Estratégia Pedagógica**
Profa. Jackeline Farbiarz

**Vice-Reitor de Infraestrutura e Serviços**
Prof. Luiz Fernando Martha

*A presente versão do documento Política de Segurança da Informação foi aprovada pelo Conselho Universitário da PUC-Rio em sessão realizada em 07/10/2025.*

# Sumário


| | |
|---|---|
| 1. ESCOPO | 06 |
| 2. CONCEITOS E DEFINIÇÕES | 06 |
| 3. REFERENCIAL NORMATIVO | 09 |
| 4. PRINCÍPIOS | 10 |
| 5. DIRETRIZES GERAIS | 10 |
| 6. COMPETÊNCIAS | 12 |
| 7. PENALIDADES | 14 |
| 8. POLÍTICA DE ATUALIZAÇÃO | 14 |
| 9. POLÍTICAS SUPLEMENTARES | 14 |

## 1. Escopo

**1.1.** A Política de Segurança da Informação (PSI) da PUC-Rio estabelece os princípios, as diretrizes, as responsabilidades e as práticas para proteger a informação de sua propriedade e/ou sob a sua guarda ou custódia legal, através da implantação de controles de segurança capazes de reduzir os riscos de segurança da informação.

**1.2.** A PSI da PUC-Rio visa assegurar:

- **i.** a segurança física dos dados da Universidade;
- **ii.** a confidencialidade, da integridade e da disponibilidade da informação;
- **iii.** a privacidade dos dados pessoais; e
- **iv.** a segurança cibernética.

**1.3.** A PSI da PUC-Rio tem o propósito de:

- **i.** atender às exigências legais e normativas aplicáveis às atividades da Universidade;
- **ii.** orientar as práticas necessárias para garantir a segurança da informação;
- **iii.** definir competências e responsabilidades; e
- **iv.** servir de referência para efeitos de auditoria.

**1.4.** A PSI da PUC-Rio se aplica a:

- **i.** todas as unidades de administração, de ensino e de pesquisa da Universidade;
- **ii.** todas as atividades institucionais dentro ou fora das instalações da Universidade;
- **iii.** todos os sistemas de informação corporativos da Universidade; e
- **iv.** todas as instalações de infraestrutura de Tecnologia da Informação e Comunicação (TIC) da Universidade.

## 2. Conceitos e definições

**2.1.** A PSI da PUC-Rio utiliza como referência, os conceitos e definições do Glossário de Segurança da Informação do GSI/PR (PORTARIA GSI/PR Nº 93, DE 18 DE OUTUBRO DE 2021), da Lei Geral de Proteção de Dados Pessoais (LGPD – LEI 13.709, DE 14 DE AGOSTO DE 2018) e do Internet Security Glossary, Version 2 (IETF RFC 4949), fazendo adequações para refletir as necessidades da Universidade.

- **i.** **ameaça:** conjunto de fatores externos com o potencial de causar em dano para um sistema ou organização;

ii. **ativos de informação:** meios de armazenamento, transmissão e processamento da informação, equipamentos necessários a isso, sistemas utilizados para tal, locais onde se encontram esses meios, recursos humanos que a eles têm acesso e conhecimento ou dado que tem valor para um indivíduo ou organização;

iii. **auditoria:** processo de exame cuidadoso e sistemático das atividades desenvolvidas, cujo objetivo é averiguar se elas estão de acordo com as disposições planejadas e estabelecidas previamente, se foram implementadas com eficácia e se estão adequadas e em conformidade à consecução dos objetivos;

iv. **autenticidade:** propriedade pela qual se assegura que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, equipamento, sistema, órgão ou entidade;

v. **confidencialidade:** propriedade pela qual se assegura que a informação não esteja disponível ou não seja revelada à pessoa, ao sistema, ao órgão ou à entidade não autorizados nem credenciados;

vi. **dado pessoal:** informação relacionada a pessoa natural identificada ou identificável;

vii. **dado pessoal sensível:** dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

viii. **disponibilidade:** propriedade pela qual se assegura que a informação esteja acessível e utilizável sob demanda por uma pessoa natural ou determinado sistema, órgão ou entidade devidamente autorizados;

ix. **encarregado de dados pessoais:** pessoa indicada pelo controlador, para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);

x. **gestor de segurança da informação:** pessoa indicada pela alta direção para realizar a gestão da segurança da informação e coordenar os trabalhos da Comissão de Gestão de Segurança da Informação, Segurança Cibernética e Proteção da Privacidade;

xi. **incidente de segurança:** qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

xii. **incidente cibernético:** ocorrência que pode comprometer, real ou potencialmente, a disponibilidade, a integridade, a confidencialidade ou a autenticidade de sistema de informação ou das informações processadas, armazenadas ou transmitidas por esse sistema. Poderá também ser caracterizado pela tentativa de exploração de vulnerabilidade de sistema de informação que caracterize violação de norma, política de segurança, procedimento de segurança ou política de uso;

xiii. **informação:** dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

xiv. **informação sensível:** informação cuja (a) divulgação, (b) alteração ou (c) destruição ou perda pode afetar adversamente os interesses ou negócios de seu proprietário ou usuário;

xv. **integridade:** propriedade pela qual se assegura que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

xvi. **irretratabilidade:** princípio de segurança da informação por meio do qual é garantido o não repúdio às informações fornecidas;

xvii. **necessidade de conhecer:** condição segundo a qual o conhecimento da informação de acesso restrito é indispensável para o adequado exercício de cargo, função, emprego ou atividade;

xviii. **privacidade:** direito de uma entidade (normalmente uma pessoa), agindo em seu próprio nome, de determinar o grau em que irá interagir com seu ambiente, incluindo o grau em que a entidade está disposta a compartilhar seus dados pessoais com terceiros;

xix. **privilégio mínimo:** conjunto mínimo de permissões necessárias em um ativo de informação para que um usuário possa realizar suas atividades de trabalho;

xx. **proteção da privacidade:** ações para assegurar a conformidade da organização com os direitos fundamentais de privacidade dos titulares de dados pessoais, conforme estabelecido pela Lei Geral de Proteção de Dados Pessoais (LGPD).

xxi. **resiliência:** capacidade de uma organização ou de uma infraestrutura de resistir aos efeitos de um incidente, ataque ou desastre, e retornar à normalidade das operações;

xxii. **risco:** no sentido amplo, trata-se da possibilidade de ocorrência de um evento que pode impactar o cumprimento dos objetivos. Pode ser mensurado em termos de impacto e de probabilidade;

xxiii. **risco de segurança da informação:** risco potencial associado à exploração de uma ou mais vulnerabilidades de um ou mais ativos de informação, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização;

xxiv. **segurança da informação:** ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

xxv. **segurança cibernética:** ações voltadas para a segurança de operações, visando garantir que os sistemas de informação sejam capazes de resistir a eventos no espaço cibernético, capazes de comprometer a disponibilida-

de, a integridade, a confidencialidade e a autenticidade dos dados armazenados, processados ou transmitidos e dos serviços que esses sistemas ofereçam ou tornem acessíveis;

**xxvi.** **tratamento:** toda operação realizada com dados pessoais, como as que se referem à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

**xxvii.** **usuários:** docentes, funcionários técnico-administrativos, terceirizados, estagiários, aprendizes, prestadores de serviço e visitantes que de alguma forma possam ter acesso a ativos de informação da organização;

**xxviii.** **violação da privacidade:** situação em que os dados pessoais são tratados em violação de um ou mais requisitos pertinentes de salvaguarda da privacidade;

**xxix.** **violação da segurança:** ação ou evento que desobedece ou de outra forma viola a política de segurança;

**xxx.** **vulnerabilidade:** condição que, quando explorada por um criminoso cibernético, pode resultar em uma violação de segurança cibernética dos sistemas computacionais ou redes de computadores, e consiste na interseção de três fatores: suscetibilidade ou falha do sistema, acesso possível à falha e capacidade de explorar essa falha.

## 3. Referencial normativo

**3.1.** As ações desenvolvidas para cumprir a PSI da PUC-Rio são norteadas pelas seguintes normas:

**i.** ABNT NBR ISO/IEC 27001:2022 – Segurança da informação, segurança cibernética e proteção à privacidade – Sistema de Gestão da Segurança da Informação (SGSI) – Requisitos;

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

**ii.** ABNT NBR ISO/IEC 27005:2023 – Segurança da informação, segurança cibernética e proteção à privacidade – Orientações para a gestão de riscos de segurança da informação.

**iii.** ABNT NBR ISO/IEC 27701:2019 – Técnicas de segurança – Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para a gestão da privacidade da informação – Requisitos e diretrizes.

## 4. Princípios

**4.1.** A PSI da PUC-Rio adota os seguintes princípios de segurança da informação:

**i.** integridade
**ii.** confidencialidade
**iii.** disponibilidade
**iv.** autenticidade
**v.** irretratabilidade
**vi.** resiliência
**vii.** privilégio mínimo
**viii.** necessidade de conhecer
**ix.** proteção da privacidade
**x.** proteção de dados pessoais

## 5. Diretrizes gerais

**5.1.** A PSI da PUC-Rio deve ser conhecida e observada por todos os funcionários técnico-administrativos, professores e colaboradores oficialmente vinculados à atuação institucional.

**5.2.** 5Os níveis gerenciais da Universidade devem zelar pelo cumprimento da PSI da PUC-Rio no âmbito de sua competência.

**5.3.** A segurança da informação deve ser entendida como uma responsabilidade coletiva.

**5.4.** A utilização dos ativos de informação da Universidade deve ser sempre compatível com a ética, confidencialidade, legalidade e finalidade das atividades institucionais.

**5.5.** Os ativos de informação da Universidade devem ser protegidos, desde sua criação até a sua destruição, com o objetivo de diminuir os riscos à violação da segurança e violação da privacidade.

**5.6.** Tratamento da Informação

**5.6.1.** Uma Política de Gestão de Informação deve ser elaborada e publicada para estabelecer a classificação dos ativos de informação e o tratamento apropriado para cada categoria de informação de acordo com o seu grau de importância.

**5.7.** Segurança Física

**5.7.1.** Uma Política de Segurança Física deve ser elaborada e publicada para assegurar a proteção das áreas que processam ou armazenam os ativos de

informação contra o acesso físico não autorizado, danos e comprometimento de informação.

**5.8.** Gestão de Ativos

**5.8.1.** A Universidade, através da Vice-Reitoria de Infraestrutura e Serviços, deve determinar as devidas responsabilidades pela proteção dos ativos e as regras de uso dos ativos.

**5.9.** Gestão de Incidentes em Segurança da Informação

**5.9.1.** A Universidade, através da Vice-Reitoria de Infraestrutura e Serviços, deve assegurar o tratamento dos incidentes de segurança da informação e das fragilidades de segurança da informação que forem notificadas.

**5.10.** Gestão dos Recursos Operacionais e de Comunicação

**5.10.1.** A operação dos sistemas de informação deve ser segura e correta.

**5.10.2.** As informações e os sistemas de informação devem ser protegidos contra as ameaças cibernéticas.

**5.10.3.** As informações danificadas ou perdidas devem ser restauradas a partir de cópias de segurança (backup).

**5.10.4.** As atividades dos usuários devem ser registradas e monitoradas em todos os sistemas de informação da Universidade.

**5.10.5.** A rede de comunicação de dados deve ser protegida e os riscos de comprometimento da informação ou interrupção dos sistemas de informação devem ser minimizados.

**5.11.** Controle de Acesso

**5.11.1.** O acesso aos sistemas de informação deve ser permitido apenas para usuários autorizados.

**5.11.2.** O acesso dos usuários autorizados deve ser permitido apenas às funcionalidades do sistema ou aplicação referentes ao seu nível de acesso.

**5.11.3.** Os usuários devem ser conscientizados sobre a responsabilidade na proteção das suas credenciais de autenticação dos sistemas de informação.

**5.12.** Gestão de Riscos

**5.12.1.** A Universidade, através da Vice-Reitoria de Infraestrutura e Serviços, deve orientar os processos de levantamento, avaliação e tratamento das vulnerabilidades e das ameaças capazes de deixar os ativos de informação em situação de risco considerada inaceitável.

**5.13.** Gestão de Continuidade

**5.13.1.** A segurança da informação deve estar incorporada na gestão de continuidade de negócio da Universidade.

**5.14.** Auditoria e Conformidade

**5.14.1.** A Universidade deve assegurar a adesão a todas as leis, normas, regulamentos e contratos relevantes para segurança da informação.

## 6. Competências

**6.1.** Compete à alta direção da Universidade:

**i.** Designar o Gestor de Segurança da Informação e os integrantes da Comissão de Gestão de Segurança da Informação, Segurança Cibernética e Proteção da Privacidade;

**ii.** Aprovar as diretrizes da PSI da PUC-Rio que vão reger as operações da Universidade, observando os requisitos do negócio, a legislação e a regulamentação;

**iii.** Aprovar o investimento financeiro, humano e material para o cumprimento das diretrizes da PSI.

**6.2.** Compete ao Gestor de Segurança da Informação:

**i.** Coordenar a Comissão de Gestão de Segurança da Informação, Segurança Cibernética e Proteção da Privacidade nos assuntos relacionados à segurança da informação;

**ii.** Coordenar a elaboração da PSI da PUC-Rio e das normas internas de segurança da informação;

**iii.** Assessorar a alta direção na implementação da PSI da PUC-Rio;

**iv.** Estimular ações de capacitação e de profissionalização de recursos humanos em temas relacionados à segurança da informação;

**v.** Incentivar estudos de novas tecnologias, bem como seus eventuais impactos relacionados à segurança da informação;

**vi.** Propor recursos necessários às ações de segurança da informação;

**vii.** Propor a execução de ações, metas e planos estratégicos relacionados à segurança da informação;

**viii.** Encaminhar periodicamente a alta direção relatórios sobre a execução dos planos e sobre os incidentes cibernéticos relevantes;

**ix.** Verificar os resultados dos trabalhos de auditoria sobre a gestão da segurança da informação; e

**x.** Comunicar tempestivamente ao encarregado de dados pessoais a ocorrência de incidentes de segurança que possam acarretar risco ou dano relevante aos titulares.

**6.3.** Compete à Comissão de Gestão de Segurança da Informação, Segurança Cibernética e Proteção da Privacidade:

- **i.** Assessorar o Gestor de Segurança da Informação na condução das ações de segurança da informação na Universidade;
- **ii.** Aprovar a execução de ações, metas e planos estratégicos relacionados à segurança da informação;
- **iii.** Analisar os relatórios sobre a execução dos planos e sobre os incidentes cibernéticos relevantes;
- **iv.** Analisar os resultados dos trabalhos de auditoria sobre a gestão da segurança da informação.

**6.4.** Compete ao encarregado de dados pessoais, no âmbito da segurança da informação, sem prejuízo das demais atribuições:

- **i.** Orientar os funcionários técnico-administrativos, professores e colaboradores oficialmente vinculados à atuação institucional sobre as práticas a serem tomadas em relação à proteção de dados pessoais; e
- **ii.** Comunicar à ANPD e ao titular dos dados pessoais a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante a esses dados.

**6.5.** Compete à Diretoria de Infraestrutura e Serviços de Tecnologia da Informação:

- **i.** Realizar o processo de gestão de risco da infraestrutura de TIC da Universidade;
- **ii.** Definir o regulamento de uso da infraestrutura de TIC da Universidade em conformidade com a PSI da PUC-Rio;
- **iii.** Documentar e reportar os incidentes de segurança da informação para a Comissão de Gestão de Segurança da Informação, Segurança Cibernética e Proteção da Privacidade.

**6.6.** Compete à Diretoria de Sistemas de Informação:

- **i.** Realizar o processo de gestão de risco dos sistemas de informação da Universidade;
- **ii.** Definir o regulamento de uso dos sistemas de informação da Universidade em conformidade com a PSI da PUC-Rio;
- **iii.** Documentar e reportar os incidentes de segurança da informação para a Comissão de Gestão de Segurança da Informação, Segurança Cibernética e Proteção da Privacidade.

**6.7.** Compete à Coordenação Central de Integridade e à Assessoria Jurídica da Reitoria:

- **i.** Assegurar a conformidade da PSI da PUC-Rio com leis, normas, regulamentos e contratos identificados como relevantes para a segurança da informação;
- **ii.** Analisar criticamente a conformidade dos sistemas de informação com a PSI da PUC-Rio;
- **iii.** Documentar e reportar os casos de não-conformidade com a PSI da PUC-Rio para a Comissão de Gestão de Segurança da Informação, Segurança Cibernética e Proteção da Privacidade.

## 7. Penalidades

**7.1.** O descumprimento das disposições estabelecidas na PSI da PUC-Rio pode ensejar a instauração de procedimento disciplinar, a depender do caso, bem como a aplicação das penalidades cabíveis, assim como de procedimento ético.

## 8. Política de atualização

**8.1.** A PSI da PUC-Rio deve ser revisada periodicamente pela Comissão de Gestão de Segurança da Informação, Segurança Cibernética e Proteção da Privacidade, em intervalo não superior a 3 (três) anos.

## 9. Políticas suplementares

O detalhamento do uso aceitável dos ativos, em áreas específicas, deve ser publicado em políticas suplementares.

PUC
RIO

voar mais alto