
 INSTITUTO ACADÊMICO DE EXCELÊNCIA	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO		PSI-001-2025
	Classificação: interna		Versão: 1.1
			Última revisão: 08/06/2025

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

1. INTRODUÇÃO.....	3
1.1. OBJETIVO.....	3
1.2. ESCOPO.....	4
2. PRINCÍPIOS DE SEGURANÇA.....	4
2.1. CONFIDENCIALIDADE.....	4
2.2. INTEGRIDADE.....	4
2.3. DISPONIBILIDADE.....	4
3. GERENCIAMENTO DE ACESSO.....	5
3.1. CONTROLE DE ACESSO.....	5
3.2. AUTENTICAÇÃO.....	5
3.3. AUTORIZAÇÃO.....	5
4. SEGURANÇA FÍSICA E AMBIENTAL.....	5
4.1. PROTEÇÃO DE INSTALAÇÕES.....	5
4.2. CONTROLE DE ACESSO FÍSICO.....	7
4.3. SEGURANÇA AMBIENTAL.....	7
5. SEGURANÇA DE REDES E COMUNICAÇÕES.....	8
5.1. PROTEÇÃO DE REDES.....	8
5.2. MONITORAMENTO E DETECÇÃO DE INTRUSÕES.....	8
5.3. USO ACEITÁVEL DE RECURSOS DE COMUNICAÇÃO.....	8
6. GESTÃO DE INCIDENTES DE SEGURANÇA.....	9
6.1. RESPOSTA A INCIDENTES.....	9
6.2. RELATÓRIOS DE INCIDENTES.....	10
7. CONSCIENTIZAÇÃO E TREINAMENTO EM SEGURANÇA.....	10
7.1. PROGRAMA DE CONSCIENTIZAÇÃO.....	10
7.2. TREINAMENTO EM SEGURANÇA.....	10
8. AVALIAÇÃO E MELHORIA CONTÍNUA.....	11
8.1. AUDITORIAS DE SEGURANÇA.....	11
8.2. REVISÃO DE POLÍTICAS E PROCEDIMENTOS.....	11
8.3. ANÁLISE DE RISCOS.....	12
8.4. MEDIÇÃO DE DESEMPENHO.....	12
9. CONFORMIDADE LEGAL E REGULATÓRIA.....	12
9.1. CONFORMIDADE COM LEIS E REGULAMENTAÇÕES.....	13
9.2. GERENCIAMENTO DE VULNERABILIDADES E PATCHES.....	13
10. RESPONSABILIDADES.....	13
10.1. DIREÇÃO.....	13
10.2. EQUIPE DE SEGURANÇA DA INFORMAÇÃO.....	14
10.3. FUNCIONÁRIOS.....	14
11. DOCUMENTOS DE REFERÊNCIA.....	14

 INSTITUTO ACADÊMICO DE EXCELÊNCIA	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO		PSI-001-2025
			Versão: 1.1
	Classificação: interna		Última revisão: 08/06/2025

1. INTRODUÇÃO

1.1. OBJETIVO

A Política de Segurança da Informação (PSI) do Instituto Acadêmico de Excelência (IAE) tem como objetivo principal estabelecer diretrizes e práticas que assegurem a confidencialidade, integridade, disponibilidade, autenticidade e legalidade das informações e sistemas críticos da organização. Isso inclui a proteção de seus ativos tangíveis e intangíveis e os recursos de tecnologia da informação e comunicação (TIC).


Ao garantir uma proteção eficaz contra ameaças cibernéticas, a PSI visa preservar a continuidade operacional, promover a conformidade com regulamentações vigentes e cultivar uma cultura de segurança entre todos os colaboradores. Assim, fortalecendo a capacidade da IAE de promover o acesso ao conhecimento e à educação, capacitando indivíduos e transformando o ser humano – conforme sua missão. Dessa forma, a política contribui para que a instituição seja reconhecida como referência em educação, inovação e inclusão, preparando líderes críticos e agentes de mudança, alinhando-se aos seus valores de inovação, ética, pesquisa, sustentabilidade, compromisso com o ensino e com a comunidade, diversidade e inclusão.

1.2. ESCOPO

Esta política se aplica a todos os funcionários, contratados, fornecedores, estudantes, professores, técnicos e parceiros que lidam direta ou indiretamente com informações e ativos da organização. Isso inclui, mas não se limita a:

- Acesso, armazenamento, processamento ou transmissão de informações institucionais;
 - Utilização de sistemas, redes, equipamentos e demais recursos de TIC fornecidos pela instituição;
- Atividades desenvolvidas em ambientes físicos e virtuais da Faculdade;
- Compartilhamento de dados e informações com terceiros, dentro dos limites legais e contratuais.

O escopo desta política visa garantir que todos os envolvidos compreendam suas responsabilidades e atuem de forma segura e ética, contribuindo para a preservação da integridade e segurança da informação em todos os níveis da organização.

 INSTITUTO ACADÊMICO DE EXCELÊNCIA	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO		PSI-001-2025
			Versão: 1.1
	Classificação: interna		Última revisão: 08/06/2025

2. PRINCÍPIOS DE SEGURANÇA

2.1. CONFIDENCIALIDADE

A confidencialidade das informações será assegurada por meio de mecanismos como criptografia de dados sensíveis, segmentação de redes e controle de acesso. Informações de alunos, professores, pesquisas acadêmicas e dados administrativos devem ser protegidas contra acessos não autorizados. O uso de VPS e comunicação segura (HTTPS, TLS) será obrigatório para acesso remoto.

2.2. INTEGRIDADE

A integridade dos dados será garantida por meio de backups frequentes, controle de versões e validação de integridade em sistemas críticos. Logs de alteração serão mantidos para sistemas acadêmicos e administrativos, assegurando rastreabilidade de modificações em históricos escolares, notas, matrículas, entre outros.

2.3. DISPONIBILIDADE

Os serviços de rede, sistemas acadêmicos e plataformas de ensino à distância deverão ter alta disponibilidade. Isso será garantido por meio de redundância de servidores, links de internet e políticas de contingência para falhas. O suporte técnico deve estar disponível em horários compatíveis com as atividades acadêmicas.


3. GERENCIAMENTO DE ACESSO

3.1. CONTROLE DE ACESSO

Implementar controles de acesso para garantir que apenas usuários autorizados possam acessar as informações e os sistemas.

Cada colaborador e aluno da Faculdade recebe uma identidade digital individual e intransferível. Essa identidade permite o acesso físico e lógico aos ambientes e recursos de Tecnologia da Informação e Comunicação (TIC), sendo monitorada e controlada pela instituição.

O uso e sigilo da identidade digital são de responsabilidade exclusiva do colaborador e do aluno. É estritamente proibido o compartilhamento, divulgação ou transferência não autorizados a terceiros.

 INSTITUTO ACADÊMICO DE EXCELÊNCIA	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PSI-001-2025
		Versão: 1.1
	Classificação: interna	Última revisão: 08/06/2025

3.2. AUTENTICAÇÃO

A autenticação dos usuários será feita através de login com senha segura e, sempre que possível, autenticação multifator (MFA). Cada aluno, professor e funcionário terá um ID único para acesso aos sistemas institucionais como AVA, e-mail e biblioteca digital.

3.3. AUTORIZAÇÃO


A autorização será baseada em perfis de acesso definidos por função (RBAC - Role-Based Access Control). Alunos, professores, coordenadores e técnicos terão permissões distintas, limitando o acesso à informações e sistemas conforme suas necessidades. O acesso a dados administrativos e sensíveis será restrito apenas a pessoal autorizado.

4. SEGURANÇA FÍSICA E AMBIENTAL

4.1. PROTEÇÃO DE INSTALAÇÕES

As estruturas destinadas a funções administrativas, acadêmicas, laboratoriais e de apoio precisam ser devidamente protegidas contra ameaças físicas – sejam violações, danos acidentais ou intencionais, sabotagem, entre outros riscos.

- 4.1.1.** O uso dos recursos de TIC (Tecnologias da Informação e Comunicação) está condicionado ao cumprimento rigoroso das normas de segurança desta Política, bem como à legislação vigente. É proibida qualquer utilização para fins pessoais, ilícitos, ou que prejudique a confidencialidade, integridade e disponibilidade das informações institucionais.
- 4.1.2.** Todos os arquivos, documentos e dados gerados nas atividades administrativas e acadêmicas devem ser armazenados exclusivamente em servidores institucionais ou repositórios oficiais, submetidos a controles de acesso, sistemas de backup e demais mecanismos de proteção.
- 4.1.3.** A aquisição, instalação, configuração, manutenção e descarte de recursos de TIC são atribuição exclusiva do setor de TI, responsável por garantir conformidade com normas internas e melhores práticas de segurança da informação.
- 4.1.4.** Todos os softwares em uso no ambiente institucional devem possuir licenciamento regular e homologação prévia pela TI. A instalação de


 INSTITUTO ACADÊMICO DE EXCELÊNCIA	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO		PSI-001-2025
			Versão: 1.1
	Classificação: interna		Última revisão: 08/06/2025

softwares não autorizados, obsoletos ou obtidos de maneira irregular é terminantemente proibida.

- 4.1.5.** Qualquer modificação em sistemas, redes ou recursos de TIC exige autorização prévia e execução exclusiva pela equipe de TI, acompanhada de registro formal para garantir rastreabilidade e redução de riscos operacionais.
- 4.1.6.** Os recursos institucionais devem dispor de controles de segurança adequados, incluindo autenticação robusta, bloqueio automático, criptografia, antivírus, firewall e monitoramento contínuo contra ameaças e softwares maliciosos.
- 4.1.7.** É expressamente proibido utilizar recursos institucionais para armazenar, transmitir ou compartilhar conteúdos ilícitos, ofensivos, discriminatórios ou incompatíveis com os objetivos da instituição.
- 4.1.8.** O uso dos recursos institucionais está sujeito a monitoramento e auditoria pela TI, visando garantir conformidade com esta Política, segurança das informações e melhoria contínua dos serviços.
- 4.1.9.** A remoção de equipamentos ou componentes de TIC das dependências do IAE só pode ocorrer mediante autorização formal da TI e do gestor responsável.
- 4.1.10.** Em caso de perda, roubo ou extravio de dispositivos institucionais que contenham informações do IAE, o responsável deve informar imediatamente a TI e a Direção da unidade, para adoção de medidas de mitigação de riscos e proteção de dados.

4.2. CONTROLE DE ACESSO FÍSICO

O acesso físico a ambientes que armazenam, processam ou transmitem informações institucionais – como data centers, laboratórios, bibliotecas, arquivos físicos, estúdios audiovisuais e áreas de rede – é restrito a pessoas formalmente autorizadas, com registro e identificação adequados.

 INSTITUTO ACADÊMICO DE EXCELÊNCIA	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PSI-001-2025
		Versão: 1.1
	Classificação: interna	Última revisão: 08/06/2025

4.2.1. Todos os colaboradores, terceiros, visitantes e prestadores de serviços que precisem acessar áreas críticas devem portar identificação visível e cumprir os procedimentos de autorização, validação e registro estabelecidos pela TI e Direção da unidade.

4.2.2. A entrada e permanência em áreas restritas sem autorização caracteriza violação grave desta Política, sujeita a sanções administrativas, civis e criminais conforme legislação vigente.

4.3. SEGURANÇA AMBIENTAL

As instalações que abrigam recursos de TI devem ser protegidas contra riscos ambientais, como incêndios, inundações e variações extremas de temperatura e umidade, por meio de sistemas de prevenção e mitigação.

4.3.1. Devem ser adotadas medidas preventivas, incluindo detectores de fumaça, sistemas de combate a incêndio adequados (extintores específicos para equipamentos elétricos), bem como climatização para garantir condições ambientais apropriadas.


4.3.2. A infraestrutura elétrica das instalações deve contar com proteção contra surtos elétricos e quedas de energia, como no-breaks e geradores, assegurando disponibilidade e continuidade dos serviços.

4.3.3. A universidade deve realizar avaliações periódicas de risco ambiental em instalações críticas, visando identificar vulnerabilidades e implementar medidas corretivas e preventivas.

5. SEGURANÇA DE REDES E COMUNICAÇÕES

5.1. PROTEÇÃO DE REDES

A organização deve implementar controles técnicos e administrativos para proteger suas redes de comunicação contra ameaças internas e externas, garantindo a confidencialidade, integridade e disponibilidade das informações trafegadas. Isso inclui o uso de firewalls, segmentação de rede, controle de acesso, criptografia e restrição de serviços não autorizados.

 INSTITUTO ACADÊMICO DE EXCELÊNCIA	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO		PSI-001-2025
	Classificação: interna		Versão: 1.1
			Última revisão: 08/06/2025

5.2. MONITORAMENTO E DETECÇÃO DE INTRUSÕES

Devem ser estabelecidos sistemas de monitoramento contínuo e de detecção/prevenção de intrusões (IDS/IPS) para identificar acessos não autorizados, falhas, comportamentos anômalos e tentativas de ataque.

Os registros de eventos devem ser armazenados e auditados periodicamente.

Incidentes identificados devem ser analisados e tratados conforme o plano de resposta a incidentes da organização.

5.3. USO ACEITÁVEL DE RECURSOS DE COMUNICAÇÃO

A seguir, definem-se as diretrizes para uso apropriado dos recursos de comunicação da organização:

5.3.1. INTERNET

O acesso à internet deve ser utilizado exclusivamente para fins institucionais. É proibido acessar conteúdos ilícitos, ofensivos ou que possam comprometer a imagem da organização. A navegação é monitorada para garantir conformidade com esta política.

5.3.2. CORREIO ELETRÔNICO


O e-mail corporativo deve ser utilizado apenas para comunicações profissionais. É proibido:

- Compartilhar senhas de acesso;
- Encaminhar mensagens fraudulentas (phishing);
- Enviar anexos suspeitos ou que contenham malware;
- Utilizar a conta institucional para fins pessoais, exceto com autorização expressa.

5.3.3. REDE SEM FIO (WI-FI)

As redes Wi-Fi da instituição devem ser protegidas com criptografia WPA2 ou superior. As senhas de acesso devem ser trocadas periodicamente e não podem ser divulgadas a pessoas não autorizadas. Portanto, visitantes devem usar redes segregadas, com acesso restrito à internet.

5.3.4. APLICATIVOS DE COMUNICAÇÃO

 INSTITUTO ACADÊMICO DE EXCELÊNCIA	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO		PSI-001-2025
			Versão: 1.1
	Classificação: interna		Última revisão: 08/06/2025

O uso de aplicativos como WhatsApp, Teams, Slack ou equivalentes deve respeitar a confidencialidade das informações institucionais. Mensagens contendo dados sensíveis não devem ser transmitidas sem autorização ou criptografia adequada.

5.3.5. MÍDIAS SOCIAIS

A utilização de mídias sociais em nome da organização deve seguir orientações específicas da área de comunicação.

- Publicações devem preservar a imagem institucional.
- É proibido divulgar informações internas ou sensíveis em ambientes públicos.

6. GESTÃO DE INCIDENTES DE SEGURANÇA

6.1. RESPOSTA A INCIDENTES

A organização deve manter um processo estruturado de resposta a incidentes de segurança da informação, com o objetivo de identificar, conter, erradicar, recuperar e aprender com eventos que possam comprometer a confidencialidade, integridade ou disponibilidade das informações e dos sistemas.

O processo deve incluir:


- Detecção e categorização do incidente;
- Notificação das partes envolvidas;
- Adoção de medidas corretivas imediatas;
- Registro detalhado do ocorrido e das ações tomadas;
- Avaliação de impacto e prevenção de recorrências.

Este processo deve estar alinhado ao plano de continuidade de negócios e ser testado periodicamente.

6.2. RELATÓRIOS DE INCIDENTES

Todos os colaboradores, prestadores de serviço e usuários autorizados devem reportar imediatamente qualquer incidente de segurança, incluindo:

- Acessos não autorizados;
- Perda ou vazamento de dados;
- Presença de malware ou comportamento suspeito em dispositivos;
- Falhas técnicas que afetem a segurança da informação.

 INSTITUTO ACADÊMICO DE EXCELÊNCIA	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO		PSI-001-2025
			Versão: 1.1
	Classificação: interna		Última revisão: 08/06/2025

Os relatos devem ser encaminhados à equipe de Segurança da Informação ou ao canal designado pela instituição. O anonimato será respeitado quando necessário, e nenhum funcionário será penalizado por comunicar incidentes de boa-fé.

7. CONSCIENTIZAÇÃO E TREINAMENTO EM SEGURANÇA

7.1. PROGRAMA DE CONSCIENTIZAÇÃO


Desenvolver e implementar um programa contínuo de conscientização para garantir que todos os funcionários e, quando aplicável, alunos, compreendam suas responsabilidades e a importância de aderir às políticas de segurança da informação.

- A conscientização será promovida via e-mails, comunicados, materiais informativos e campanhas.
- Temas incluem: identificação de ameaças (phishing, malware), uso seguro de senhas, manuseio de dados confidenciais, política de uso aceitável de TI e relato de incidentes.
- O conteúdo será revisado anualmente ou mediante mudanças em políticas ou ameaças.

7.2. TREINAMENTO EM SEGURANÇA

Fornecer treinamento regular e direcionado em segurança da informação, mantendo funcionários e usuários relevantes atualizados sobre melhores práticas, políticas internas e tecnologias de proteção.

- Treinamento Inicial: Novos funcionários e colaboradores com acesso a sistemas e dados devem concluir treinamento básico antes do início das atividades.
- Treinamento Periódico: Treinamentos periódicos (mínimo anual) serão oferecidos a todos os funcionários, abordando atualizações sobre ameaças e políticas.
- Treinamento Específico: Treinamentos específicos serão desenvolvidos para equipes que lidam com dados sensíveis, sistemas críticos ou funções de alto risco (ex: TI, RH, secretarias).
- Formatos incluem presenciais, online (e-learning) ou workshops.
- O registro de participação será mantido para conformidade e auditoria.

 INSTITUTO ACADÊMICO DE EXCELÊNCIA	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO		PSI-001-2025
			Versão: 1.1
	Classificação: interna		Última revisão: 08/06/2025

8. AVALIAÇÃO E MELHORIA CONTÍNUA

A organização compromete-se com a **melhoria contínua** de seus controles e práticas de segurança da informação, buscando garantir a eficácia das medidas adotadas e a adequação frente às mudanças tecnológicas e ao cenário de ameaças.

8.1. AUDITORIAS DE SEGURANÇA

Devem ser realizadas **auditorias de segurança periódicas** para avaliar o cumprimento das políticas, normas e procedimentos de segurança da informação.

Essas auditorias visam:

- Verificar a conformidade com requisitos legais e regulatórios;
- Identificar vulnerabilidades ou falhas de controle;
- Recomendar ações corretivas e de prevenção.

As auditorias podem ser conduzidas por equipes internas ou externas, conforme a criticidade dos sistemas auditados.

8.2. REVISÃO DE POLÍTICAS E PROCEDIMENTOS

As **políticas e procedimentos de segurança** devem ser revisados e atualizados regularmente, levando em consideração:


- Evolução tecnológica;
- Novas ameaças identificadas;
- Mudanças legais ou regulatórias;
- Resultados de auditorias e incidentes anteriores.

A revisão deve ocorrer ao menos uma vez por ano ou sempre que houver mudanças significativas no ambiente institucional.

8.3. ANÁLISE DE RISCOS

Devem ser conduzidas **análises de risco** de forma periódica para identificar, classificar e tratar os riscos relacionados aos ativos de informação da organização.

O processo deve incluir:

 INSTITUTO ACADÊMICO DE EXCELÊNCIA	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PSI-001-2025
		Versão: 1.1
	Classificação: interna	Última revisão: 08/06/2025

- Identificação de ameaças e vulnerabilidades;
- Avaliação do impacto e da probabilidade;
- Definição de medidas de mitigação e planos de tratamento.

Os resultados devem orientar decisões estratégicas e operacionais no âmbito da segurança da informação.

8.4. MEDIÇÃO DE DESEMPENHO

Devem ser definidos e acompanhados **indicadores-chave de desempenho (KPIs)** para mensurar a eficácia dos controles e programas de segurança.

Esses indicadores devem permitir:

- Avaliação objetiva da maturidade da segurança da informação;
- Detecção de desvios e pontos de melhoria;
- Suporte à tomada de decisão da alta gestão.


A medição de desempenho deve estar integrada ao ciclo de melhoria contínua da instituição.

9. CONFORMIDADE LEGAL E REGULATÓRIA

A Política de Segurança da Informação do instituto deve estar alinhada às obrigações legais e regulatórias vigentes, assegurando que todas as práticas e controles de segurança adotados estejam em conformidade com as leis aplicáveis, especialmente aquelas relacionadas à privacidade e proteção de dados pessoais. Além disso, a instituição deve adotar medidas proativas para mitigar vulnerabilidades técnicas e garantir a integridade dos seus sistemas de informação.

9.1. CONFORMIDADE COM LEIS E REGULAMENTAÇÕES

Todas as atividades relacionadas à segurança da informação devem estar em conformidade com as legislações e regulamentações aplicáveis, incluindo, mas não se limitando à Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 – LGPD), ao Marco Civil da Internet (Lei nº 12.965/2014) e demais normas pertinentes ao setor público e educacional. O instituto se compromete a revisar periodicamente suas políticas, processos e controles de segurança, de modo a

	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PSI-001-2025
		Versão: 1.1
	Classificação: interna	Última revisão: 08/06/2025

garantir sua aderência às exigências legais, promovendo a transparência, o uso ético das informações e a proteção dos direitos dos titulares de dados.

9.2. GERENCIAMENTO DE VULNERABILIDADES E PATCHES


A universidade deverá implementar um processo contínuo de identificação, avaliação e correção de vulnerabilidades nos sistemas, aplicações e dispositivos conectados à rede institucional. Isso inclui o monitoramento constante de falhas conhecidas, a realização de análises de risco e a aplicação regular de atualizações e patches de segurança fornecidos por fabricantes e desenvolvedores. Os serviços críticos da instituição, como o servidor web, o sistema acadêmico para estudantes e professores, o sistema da biblioteca, os serviços de banco de dados, DNS, FTP, NFS, Proxy e Cache, devem ser constantemente avaliados quanto à presença de vulnerabilidades e mantidos atualizados com as correções necessárias. A gestão de vulnerabilidades deve ser feita de forma planejada e controlada, minimizando impactos operacionais e garantindo a continuidade, a disponibilidade e a segurança dos serviços essenciais à comunidade acadêmica.

10. RESPONSABILIDADES

Esta PSI é um normativo interno, com valor jurídico e aplicabilidade imediata e irrestrita a todos os alunos e colaboradores, para os ambientes estudantil, acadêmico e administrativo, que venham a ter acesso e/ou utilizam as informações, os recursos de TIC e/ou demais ativos tangíveis ou intangíveis da SMC e mantidas.

10.1. DIREÇÃO

A alta direção da instituição é responsável por aprovar, promover e revisar periodicamente a Política de Segurança da Informação. Cabe à direção garantir que os recursos necessários — humanos, tecnológicos e financeiros — estejam disponíveis para a implementação e manutenção das medidas de segurança. Além disso, a direção deve assegurar o alinhamento da PSI com os objetivos estratégicos da IAE e com a legislação vigente, como a Lei Geral de Proteção de Dados (LGPD), reforçando o compromisso institucional com a governança da informação.

	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PSI-001-2025
		Versão: 1.1
	Classificação: interna	Última revisão: 08/06/2025

10.2. EQUIPE DE SEGURANÇA DA INFORMAÇÃO

A equipe de segurança da informação tem como responsabilidade principal planejar, executar, monitorar e realizar a manutenção das políticas e práticas de segurança previstas na PSI. Suas atribuições incluem a identificação de riscos, definição de controles, resposta a incidentes de segurança e a promoção contínua de campanhas de conscientização. Essa equipe também deve manter a documentação atualizada, realizar auditorias internas e reportar periodicamente à direção os indicadores e resultados obtidos na gestão da segurança da informação.

10.3. FUNCIONÁRIOS

Todos os funcionários do Instituto Acadêmico de Excelência — sejam administrativos, técnicos ou docentes — devem conhecer e cumprir as diretrizes estabelecidas nesta política. Cada colaborador é responsável por zelar pela segurança das informações com as quais lida, reportar situações suspeitas ou incidentes à equipe de segurança, além de seguir as boas práticas definidas na cartilha de acesso seguro. O comprometimento individual com a segurança da informação é fundamental para proteger os dados institucionais e manter a confiabilidade dos serviços oferecidos pela universidade.

11. DOCUMENTOS DE REFERÊNCIA

O presente documento será complementado pelos Códigos e Normas de Segurança da Informação do Instituto Acadêmico de Excelência e está em consonância com os seguintes documentos:

- ABNT NBR ISO/IEC 27001:2013 – Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos;
- ABNT NBR ISO/IEC 27002:2013 – Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação;
- ABNT NBR ISO/IEC 27014:2013 – Tecnologia da informação — Técnicas de segurança — Governança de segurança da informação.