UNIVERSIDADE POLARIS

Instituto de Segurança da Informação

Política de Segurança

Colaboradores: Davih Gonçalves Duque, Fabiana Santos Soares, Filipe Acacio Costa, Leonardo Guedes Gomes Junior, Vítor César Reis Francisco, Lucas de Oliveira Fonseca

Belo Horizonte — Minas Gerais

2025

1 INTRODUÇÃO

1.1. OBJETIVO

Esta Política de Segurança da Informação (PSI) tem como finalidade estabelecer as diretrizes, princípios e responsabilidades que orientam a proteção dos ativos informacionais da Universidade Polaris, assegurando o uso ético, seguro e alinhado aos valores institucionais.

A PSI busca garantir que todos os processos e atividades da Universidade — acadêmicos, administrativos e de pesquisa — sejam sustentados por práticas que promovam a confidencialidade, a integridade e a disponibilidade das informações, prevenindo incidentes e fortalecendo a confiança da comunidade universitária no ambiente digital.

Além disso, visa fomentar uma cultura de segurança da informação entre colaboradores, docentes, discentes e parceiros, estimulando a conscientização e a corresponsabilidade no uso adequado dos recursos sob gestão da instituição.

1.2. ESCOPO

Esta Política aplica-se a todos os colaboradores, docentes, discentes, prestadores de serviço, fornecedores e parceiros que, de forma direta ou indireta, tenham acesso, manipulem ou armazenem informações e ativos sob responsabilidade da Universidade Polaris.

O cumprimento das diretrizes aqui estabelecidas é obrigatório para todos que utilizam os sistemas, redes e dados institucionais, independentemente do vínculo ou nível de acesso.

A abrangência inclui todos os ambientes físicos e digitais da Universidade, compreendendo infraestrutura de TI, aplicações, plataformas acadêmicas, ambientes administrativos e quaisquer outros sistemas que integrem o ecossistema informacional da instituição.

2. PRINCÍPIOS DE SEGURANÇA

2.1. CONFIDENCIALIDADE

A confidencialidade deve ser garantida por meio de controles que limitem o acesso às informações apenas a indivíduos devidamente autorizados, protegendo dados institucionais contra divulgação indevida.

Os acessos devem ser atribuídos conforme necessidade, seguindo políticas de autenticação e autorização, além de mecanismos que impeçam o compartilhamento não autorizado de credenciais. Informações sensíveis devem ser armazenadas e transmitidas utilizando métodos que assegurem sua proteção.

2.2. INTEGRIDADE

A integridade das informações será preservada por meio de mecanismos que assegurem que dados e sistemas permaneçam completos, precisos e livres de alterações não autorizadas. A implementação de registros de auditoria, validação de configurações, controle de versões e monitoramento contínuo contribui para detectar alterações indevidas e garantir que as informações refletem o estado real dos processos institucionais. Procedimentos de revisão devem ser aplicados sempre que houver riscos de modificação ou inconsistência.

2.3. DISPONIBILIDADE

A disponibilidade dos sistemas e recursos de TI será mantida por meio de práticas que assegurem seu funcionamento contínuo, garantindo acesso sempre que necessário para atividades acadêmicas e administrativas. A utilização de serviços redundantes, monitoramento constante dos componentes da infraestrutura e políticas de recuperação em caso de falhas são essenciais para minimizar interrupções.

Manutenções preventivas e revisões periódicas devem ser realizadas para garantir estabilidade e resposta eficiente a incidentes que possam comprometer o acesso aos serviços.

3. GERENCIAMENTO DE ACESSO

3.1. CONTROLE DE ACESSO

O controle de acesso na Universidade Polaris é estruturado conforme níveis hierárquicos e critérios de necessidade, assegurando que apenas usuários devidamente autorizados acessem os sistemas, informações e recursos tecnológicos institucionais.

O modelo interno segue uma pirâmide de acesso:

- **Nível Administrativo** – Acesso ampliado, destinado à Direção, Coordenação e setores de gestão que demandam informações estratégicas e operacionais;
- **Nível Docente** – Acesso intermediário, voltado à execução de atividades pedagógicas e à gestão de turmas;
- **Nível Colegiado** – Acesso restrito, limitado às ferramentas e informações necessárias às atividades acadêmicas dos estudantes.

Os acessos concedidos a visitantes, fornecedores e prestadores de serviço são temporários e controlados, exigindo autorização prévia de um responsável institucional e limitando-se ao período e aos recursos estritamente necessários à execução das atividades. Após o término da necessidade, esses acessos devem ser imediatamente revogados.

Todos os acessos, internos ou externos, devem seguir o princípio do menor privilégio, sendo obrigatoriamente registrados, auditáveis e revisados periodicamente, a fim de preservar a integridade, a confidencialidade e a disponibilidade das informações institucionais.

3.2. AUTENTICAÇÃO

Os processos de autenticação devem garantir que o acesso aos sistemas, redes e informações seja realizado exclusivamente por usuários devidamente identificados e autorizados.

A autenticação ocorre mediante credenciais individuais e intransferíveis, assegurando a rastreabilidade de todas as ações executadas em ambiente digital. É estritamente proibido o compartilhamento de contas, senhas ou dispositivos de autenticação.

Sempre que tecnicamente viável, devem ser utilizados métodos de autenticação multifator (MFA), combinando senhas, tokens, chaves digitais ou outros mecanismos que reforcem a segurança e reduzam o risco de acessos indevidos.

A configuração do processo de autenticação deve considerar a sensibilidade das informações e o nível de acesso do usuário, aplicando camadas adicionais de proteção a perfis administrativos e sistemas críticos.

As credenciais de visitantes, fornecedores e prestadores de serviço devem possuir prazo de validade definido e autorização prévia do responsável pela área solicitante, sendo automaticamente revogadas ao término da atividade.

3.3. AUTORIZAÇÃO

Os níveis de autorização devem ser definidos conforme as funções e responsabilidades de cada usuário, garantindo o acesso estritamente necessário ao desempenho das atividades institucionais, em conformidade com o princípio do menor privilégio.

As permissões devem ser revisadas sempre que houver mudança de função, desligamento ou transferência de área.

O acesso a informações classificadas como sensíveis ou críticas requer autorização formal do responsável pela área gestora, acompanhado de registro para fins de auditoria e rastreabilidade.

Os acessos temporários – destinados a visitantes, fornecedores e prestadores de serviço – devem possuir validade definida, ser monitorados durante seu uso e revogados imediatamente após o término da necessidade operacional.

Qualquer exceção aos critérios de autorização deve ser formalmente documentada e aprovada pela equipe responsável pela Segurança da Informação.

4. SEGURANÇA FÍSICA E AMBIENTAL

4.1. PROTEÇÃO DE INSTALAÇÕES

O ambiente físico da Instituição deve ser projetado, mantido e monitorado de forma a garantir que os ativos e equipamentos de tecnologia da informação sejam resguardados contra ameaças físicas, como roubo, vandalismo ou danos acidentais. Isso inclui a instalação de sistemas de videovigilância em pontos estratégicos, bem como a utilização de portas reforçadas, fechaduras de alta segurança e móveis trancados para o alojamento de equipamentos críticos. Deve-se registrar e controlar o ingresso de visitantes, prestadores de serviços e terceiros, exigindo-se identidade, autorização e supervisão permanente durante sua permanência nas áreas sensíveis. É recomendada a utilização de sinalização clara para delimitar zonas restritas, bem como a adoção de barreiras físicas (grades, catracas, biometria) adequadas ao nível de risco identificado, garantindo a integridade dos espaços vitais à tecnologia da informação.

4.2. CONTROLE DE ACESSO FÍSICO

O acesso físico às áreas críticas – como salas de servidores, salas de rede e laboratórios restritos – deve estar sujeito a controle rigoroso, com concessão restrita a indivíduos autorizados e devidamente identificados. Para tal, devem ser adotados dispositivos de autenticação (cartões de acesso, chaves codificadas, biometria), bem como um sistema de registro de entradas e saídas que permita auditoria das movimentações. O acesso temporário somente poderá ser concedido mediante autorização formal, e deverá ser revogado imediatamente em caso de desligamento, mudança de função ou término de atividade. Os registros devem ser periodicamente revisados e auditados para identificação de acessos indevidos ou suspeitos, assegurando a rastreabilidade e oferta de evidências para investigações caso necessário.

4.3. SEGURANÇA AMBIENTAL

É imperativo proteger a infraestrutura de tecnologia da informação contra os riscos ambientais que possam comprometer a disponibilidade, integridade ou confidencialidade dos serviços.

Deve-se implementar sistemas de climatização apropriados para manter a temperatura e a umidade dentro dos parâmetros pré-definidos para o funcionamento seguro dos equipamentos.

A instalação de sensores de temperatura, fumaça, umidade ou vazamento de água, com alertas automáticos atrelados a plano de resposta emergencial, é fundamental. Além disso, a adoção de fontes de energia redundantes (nobreaks, geradores) e filtros contra surtos elétricos, bem como aterramento adequado, constituem medidas essenciais para garantir continuidade operacional. Em paralelo, devem ser previstos sistemas de combate a incêndio compatíveis com o ambiente de TI (por exemplo, extintores de gás inerte, detectores automáticos), bem como planos de contingência para desastres naturais, enchentes, falhas críticas de energia ou outras emergências que possam afetar os ambientes físicos.

5. CLASSIFICAÇÃO DA INFORMAÇÃO

A classificação da informação na Universidade Polaris define níveis de sensibilidade que orientam o acesso, o armazenamento e o compartilhamento de dados institucionais. Essa categorização assegura que cada tipo de informação receba o grau adequado de proteção, reduzindo riscos associados ao uso indevido, vazamentos ou manipulações não autorizadas.

A instituição utiliza quatro categorias principais:

- **Pública** – Informações de livre acesso, cuja divulgação externa não representa risco institucional.
- **Interna** – Dados destinados ao uso de colaboradores, cuja exposição pode gerar impactos operacionais moderados.
- **Confidencial** – Informações pessoais, acadêmicas ou administrativas que exigem controle rigoroso de acesso e registro de atividades.
- **Restrita** – Conteúdos altamente sensíveis, capazes de causar danos significativos em caso de exposição, exigindo proteção reforçada.

5.1. REGRAS DE TRATAMENTO POR NÍVEL DE CLASSIFICAÇÃO

O tratamento das informações deve obedecer à classificação atribuída, assegurando sua proteção desde a criação até o descarte. Cada categoria requer controles específicos de acesso, armazenamento e transmissão, de forma a preservar a integridade, a confidencialidade e a disponibilidade dos dados institucionais.

Documentos e registros considerados restritos ou confidenciais devem ser armazenados em sistemas ou repositórios protegidos, acessíveis apenas a usuários autorizados. Seu compartilhamento deve ser limitado aos responsáveis pelas atividades correspondentes e deve ocorrer por meios seguros. Informações classificadas como internas devem circular apenas no ambiente institucional, enquanto dados públicos podem ser divulgados sem restrições adicionais. Todos os procedimentos devem estar alinhados às normas institucionais e às leis aplicáveis sobre proteção de dados.

6. SEGURANÇA DE REDES E COMUNICAÇÕES

6.1. PROTEÇÃO DE DADOS

Os serviços de rede foram configurados de maneira a garantir a proteção das informações trafegadas entre servidores e usuários, assegurando que todos os componentes da infraestrutura operassem de forma segura e confiável.

A proteção dos dados será assegurada por meio da manutenção de registros e auditorias dos serviços críticos, possibilitando a identificação de alterações indevidas, acessos não autorizados e comportamentos fora do padrão.

Todas as modificações realizadas nos serviços de rede serão registradas e revisadas, garantindo continuidade operacional, padronização das configurações e conformidade com as diretrizes de segurança da instituição.

6.2. MONITORAMENTO E DETECÇÃO DE INTRUSÕES

Os serviços essenciais da infraestrutura serão monitorados continuamente, permitindo identificar falhas, comportamentos anômalos e possíveis tentativas de intrusão. Esses indicadores permitem detectar situações de sobrecarga, indisponibilidade ou variações anormais de tráfego que possam representar riscos à segurança da infraestrutura.

Alertas e registros gerados pelo sistema serão analisados de forma sistemática, possibilitando resposta imediata a incidentes que comprometam a estabilidade ou a integridade das comunicações. Os dados coletados serão preservados para auditoria e investigação, garantindo rastreabilidade e eficácia nos processos de detecção de ameaças.

Todas as atividades de monitoramento e auditoria serão mantidas com registros atualizados, assegurando que desvios e incidentes sejam rastreáveis e tratados conforme os procedimentos institucionais.

7. GESTÃO DE INCIDENTES DE SEGURANÇA

7.1. RESPOSTA A INCIDENTES

A Instituição mantém um processo formalizado de resposta a incidentes para garantir tratamento ágil e documentado de eventos de segurança.

Este processo engloba, obrigatoriamente, as etapas de identificação, classificação, contenção, erradicação, recuperação e análise pós-incidente. Compete à equipe de Segurança da Informação, ao detectar ou ser notificada de uma ameaça, realizar a priorização e avaliação de impacto imediata, executando as contramedidas necessárias para impedir a propagação do incidente.

Durante a fase de resposta, a equipe técnica deve assegurar a preservação de logs e evidências digitais para fins de auditoria, investigação interna ou colaboração com autoridades competentes.

Após a restauração dos serviços e o retorno à normalidade operacional, deve ser conduzida uma análise de causa-raiz para implementar ações corretivas e propor melhorias nos controles de segurança, visando prevenir a reincidência.

7.2. RELATÓRIOS DE INCIDENTES

É dever de todos os colaboradores, docentes, discentes e prestadores de serviço comunicar imediatamente à equipe de Segurança da Informação qualquer ocorrência ou suspeita de incidente, incluindo, mas não se limitando a: acessos não autorizados, falhas operacionais, violação de dados ou perda de ativos.

As comunicações devem ser formalizadas através dos canais oficiais da instituição, preferencialmente pelo endereço eletrônico específico (ex: incidentes.seguranca@polaris.edu.br), para garantir a rastreabilidade do chamado.

O registro do incidente deve conter, minimamente: data e hora da ocorrência, descrição detalhada do fato, identificação dos envolvidos (se conhecidos), impactos observados e medidas preliminares adotadas.

Em casos específicos de furto, roubo ou perda de dispositivos institucionais (notebooks, tablets, smartphones) ou particulares que contenham dados da Universidade Polaris, o usuário responsável deve registrar um Boletim de Ocorrência (B.O.) junto ao órgão de segurança pública competente e encaminhar uma cópia imediatamente à equipe de Segurança da Informação. Todos os registros de incidentes serão mantidos em base de dados segura para fins de auditoria, conformidade com a Lei Geral de Proteção de Dados (LGPD) e aprimoramento contínuo das estratégias de defesa cibernética da instituição.

8. CONSCIENTIZAÇÃO E TREINAMENTO EM SEGURANÇA

8.1. PROGRAMA DE CONSCIENTIZAÇÃO

Fica instituído o Programa de Conscientização em Segurança da Informação, de caráter permanente, sob responsabilidade da área de Segurança da Informação em conjunto com a Comunicação Interna. O programa tem por objetivo disseminar a cultura de proteção de dados, alertar sobre ameaças emergentes e reforçar as diretrizes desta Política junto à comunidade acadêmica e administrativa.

As ações de conscientização serão realizadas periodicamente através dos canais de comunicação institucional, abrangendo docentes, discentes, colaboradores e terceiros.

Cabe a cada usuário a leitura e a observância dos materiais divulgados como a cartilha de segurança da informação, devendo aplicar as boas práticas recomendadas na execução de suas atividades rotineiras e na utilização dos recursos de TIC da instituição.

8.2. TREINAMENTO EM SEGURANÇA

A capacitação em Segurança da Informação é obrigatória para todos os colaboradores e docentes da Universidade Polaris, sendo requisito fundamental para a concessão e manutenção de acessos aos sistemas corporativos.

Treinamento Introdutório: Todo novo colaborador, no ato de sua admissão ou integração, deverá realizar o treinamento básico sobre a Política de Segurança da Informação e assinar o respectivo Termo de Ciência e Responsabilidade. A liberação definitiva das credenciais de acesso (identidade digital) está condicionada à conclusão desta etapa.

Reciclagem: Serão realizados ciclos de atualização e reciclagem, com periodicidade definida pela equipe de Segurança da Informação, para garantir que os colaboradores estejam alinhados às mudanças legislativas e às novas tecnologias de proteção.
A área de Gestão de Pessoas (RH) manterá o registro histórico da participação dos colaboradores nos treinamentos, para fins de auditoria e comprovação de conformidade legal.

9. AVALIAÇÃO E MELHORIA CONTÍNUA

9.1. AUDITORIAS DE SEGURANÇA

A Instituição submeterá seus ambientes, sistemas e processos a auditorias de segurança periódicas, com o objetivo de verificar a conformidade com esta Política, as normas internas e a legislação vigente.

As auditorias poderão ser realizadas por equipe interna independente ou por consultoria externa especializada, devendo ocorrer em intervalos planejados ou quando houver mudanças significativas na infraestrutura tecnológica.

Os relatórios de auditoria, contendo as não conformidades identificadas e as oportunidades de melhoria, devem ser apresentados à Alta Direção. As áreas auditadas têm o dever de elaborar e cumprir planos de ação para correção dos apontamentos dentro dos prazos estipulados.

9.2. REVISÃO DE POLÍTICAS E PROCEDIMENTOS

Esta Política e os procedimentos de segurança correlatos devem ser revisados, no mínimo, anualmente, ou em intervalos menores caso ocorram eventos críticos, tais como:

- Mudanças significativas na infraestrutura de TIC ou no negócio;
- Ocorrência de incidentes de segurança de alto impacto;
- Alterações na legislação aplicável (ex: LGPD).

A revisão tem por finalidade garantir a adequação, suficiência e eficácia das normas frente às novas ameaças e à evolução tecnológica. As atualizações devem ser aprovadas pelo Comitê de Segurança da Informação antes de sua publicação.

9.3. ANÁLISE DE RISCOS

A Universidade Polaris deve manter um processo estruturado de Gestão de Riscos, alinhado às melhores práticas de mercado (como a norma ISO 27005), para identificar, analisar e avaliar as ameaças aos ativos de informação.

A análise de riscos deve considerar a probabilidade de ocorrência de ameaças e o impacto potencial nos pilares de confidencialidade, integridade e disponibilidade. Com base nos resultados, devem ser definidos planos de tratamento dos riscos (mitigação, transferência, evitação ou aceitação), priorizando os recursos de proteção para os ativos mais críticos.

9.4. MEDIÇÃO DE DESEMPENHO

Fica estabelecida a necessidade de definição de métricas e Indicadores-Chave de Desempenho (KPIs) para mensurar a eficácia dos controles de segurança implementados.

A equipe de Segurança da Informação deve elaborar relatórios gerenciais periódicos, apresentando a evolução dos indicadores (ex: número de incidentes, tempo de resposta, percentual de colaboradores treinados) para subsidiar a tomada de decisão estratégica e garantir o alinhamento da segurança com os objetivos educacionais da instituição.

10. CONFORMIDADE LEGAL E REGULATÓRIA

10.1. CONFORMIDADE COM LEIS E REGULAÇÕES

A Universidade Polaris deve assegurar que todas as práticas, processos, sistemas e atividades relacionadas à segurança da informação estejam plenamente alinhados às legislações vigentes, normas regulatórias e padrões aplicáveis ao tratamento de dados e proteção de ativos institucionais.

Entre as regulamentações obrigatórias estão, mas não se limitam a:

Lei Geral de Proteção de Dados (LGPD – Lei 13.709/2018), que rege o tratamento de dados pessoais em território nacional.

Normas de direitos autorais, especialmente em ambientes acadêmicos.
Regulamentações de órgãos governamentais aplicáveis ao setor educacional.
Normas técnicas de segurança da informação amplamente reconhecidas, como referências da ISO/IEC 27001 e 27002.

Informações sejam coletadas, armazenadas, compartilhadas e descartadas de acordo com recomendações legais e boas práticas de segurança.

Cabe à Universidade Polaris assegurar a atualização contínua das políticas internas, acompanhando mudanças legais e normativas que impactem seus processos de segurança da informação.

10.2. GERENCIAMENTO DE VULNERABILIDADES E PATCHES

A Universidade Polaris deve manter um processo contínuo e sistemático para identificação, avaliação, tratamento e correção de vulnerabilidades relacionadas aos seus sistemas, dispositivos, aplicações e infraestrutura tecnológica.

Este processo deve incluir:

Monitoramento proativo de vulnerabilidades divulgadas por fabricantes, entidades de segurança e órgãos especializados.

Execução periódica de varreduras (scans) em servidores, redes, dispositivos e serviços expostos, para identificação de brechas e riscos operacionais.

Classificação das vulnerabilidades com base no impacto, probabilidade e criticidade, priorizando correções que possam afetar informações sensíveis ou sistemas essenciais à operação da Instituição.

Aplicação de patches e atualizações de segurança de maneira controlada, documentada e testada, evitando indisponibilidades e garantindo a integridade dos sistemas.

O gerenciamento eficaz de vulnerabilidades contribui diretamente para reduzir riscos operacionais, prevenir incidentes e reforçar a postura de segurança da Universidade Polaris.

11. RESPONSABILIDADES

11.1. DIREÇÃO

A Direção da Universidade Polaris é responsável por fornecer o suporte institucional necessário para a consolidação da Política de Segurança da Informação. Isso inclui:
Aprovar e divulgar oficialmente esta política.
Garantir que haja recursos financeiros, tecnológicos e humanos suficientes para sua implementação.
Promover uma cultura organizacional voltada à proteção das informações.
Zelar pelo cumprimento das obrigações legais, regulatórias e contratuais.
Assegurar que a área de Segurança da Informação possua autonomia e autoridade para executar suas atribuições.
A Direção deve ainda revisar periodicamente os indicadores e resultados do programa de segurança, assegurando que os objetivos estratégicos da Instituição sejam atendidos.

11.2. EQUIPE DE SEGURANÇA DA INFORMAÇÃO

A equipe de Segurança da Informação é responsável por implementar, monitorar e aprimorar os controles definidos nesta Política, incluindo:
Administrar e supervisionar os processos de gestão de riscos, incidentes, vulnerabilidades e conformidade.
Definir diretrizes técnicas e orientações para proteção dos ativos informacionais.
Monitorar continuamente redes, sistemas e serviços, garantindo detecção precoce de ameaças ou anomalias.
Coordenar respostas a incidentes de segurança, assegurando comunicação rápida e eficaz aos setores envolvidos.
Elaborar e conduzir programas de conscientização e treinamentos.
Cabe à equipe garantir a execução alinhada das melhores práticas de segurança, atuando de forma preventiva e responsiva frente a ameaças.

11.3. FUNCIONÁRIOS

Todos os funcionários, colaboradores, docentes, discentes, terceirizados e prestadores de serviço da Universidade Polaris têm responsabilidade direta e individual pela proteção das informações às quais têm acesso.

Cada usuário deve:

Cumprir integralmente todas as diretrizes estabelecidas nesta PSI.

Utilizar sistemas e recursos tecnológicos apenas para fins institucionais e de acordo com os níveis de acesso definidos.

Proteger credenciais de acesso, mantendo sigilo e não compartilhando senhas ou dispositivos de autenticação.

A participação ativa dos funcionários é fundamental para preservar a confidencialidade, a integridade e a disponibilidade dos ativos informacionais, garantindo que a Universidade Polaris mantenha um ambiente seguro para ensino, pesquisa e administração.