


| | | |
|---|--|---------------------------------------|
|  | POLÍTICA DE SEGURANÇA DA INFORMAÇÃO | PSI-001-2025 |
| | | VERSÃO: 1.1 |
| | CLASSIFICAÇÃO: INTERNA | ÚLTIMA REVISÃO: 08/06/2025 |

| | |
|--|-----------|
| 1. INTRODUÇÃO | 3 |
| 1.1. Objetivo | 3 |
| 1.2. Escopo | 3 |
| 2. PRINCÍPIOS DE SEGURANÇA | 3 |
| 2.1. Confidencialidade | 3 |
| 2.2. Integridade | 4 |
| 2.3. Disponibilidade | 4 |
| 2.4. Legalidade | 4 |
| 3. GERENCIAMENTO DE ACESSO | 4 |
| 3.1. Controle de Acesso | 4 |
| 3.3. Autorização | 5 |
| 4. SEGURANÇA FÍSICA E AMBIENTAL | 5 |
| 4.1. Proteção de instalações | 5 |
| 4.2. Controle de acesso físico | 6 |
| 4.3. Segurança ambiental | 6 |
| 5. SEGURANÇA DE REDES E COMUNICAÇÕES | 6 |
| 5.1. Proteção de redes | 6 |
| 5.2. Monitoramento e detecção de intrusões | 7 |
| 6.1. Resposta a incidentes | 7 |
| 7. CONSCIENTIZAÇÃO E TREINAMENTO EM SEGURANÇA | 8 |
| 7.1. Programa de conscientização | 8 |
| 7.2. Treinamento em segurança | 9 |
| 8. AVALIAÇÃO E MELHORIA CONTÍNUA | 9 |
| 8.1. Auditorias de segurança | 9 |
| 8.2. Revisão de políticas e procedimentos | 9 |
| 8.3. Análise de riscos | 10 |
| 8.4. Medição de desempenho | 10 |
| 9. CONFORMIDADE LEGAL E REGULATÓRIA | 10 |
| 9.1. Conformidade com leis e regulamentações | 10 |
| 10. RESPONSABILIDADES | 11 |
| 10.1. Direção Geral e Reitoria | 11 |
| 10.2. Equipe de TI | 12 |
| 10.3. Gestores de Área | 12 |
| 10.4. Usuários | 12 |

| | |
|-------------------|----|
| 10.4. Penalidades | 12 |
| 11. GLOSSÁRIO | 12 |

1. Introdução

A Universidade Nova Horizonte é uma instituição de ensino superior comprometida com a excelência acadêmica, a formação humanística e o desenvolvimento social, oferecendo cursos de graduação, pós-graduação e programas de extensão voltados à construção do conhecimento em todo o território nacional. Integrando inovação e responsabilidade, a universidade adota tecnologias educacionais e soluções digitais para viabilizar o acesso à educação de qualidade, independentemente de fronteiras geográficas.

Neste cenário cada vez mais digital e interconectado, a segurança da informação torna-se um elemento estratégico e indispensável para garantir a proteção de ativos essenciais — tangíveis e intangíveis — como a imagem institucional, o patrimônio tecnológico, os dados acadêmicos e administrativos, as pesquisas científicas e a confiança da comunidade universitária.

A crescente dependência de sistemas informatizados, ambientes em nuvem, plataformas de ensino remoto e serviços digitais exige que todos os usuários — sejam da esfera administrativa, acadêmica ou de apoio — atuem de forma responsável e consciente na preservação da segurança das informações. Isso implica em adotar práticas seguras, respeitar os controles estabelecidos, compreender os riscos e colaborar para um ambiente digital íntegro, confiável e resiliente.

Esta Política de Segurança da Informação (PSI) é, portanto, um instrumento institucional que orienta o uso adequado, ético e legal dos ativos informacionais da universidade, promovendo a conformidade com as leis vigentes, a prevenção de riscos e a continuidade das atividades educacionais e administrativas.

1.1. Objetivo

O objetivo desta política é estabelecer diretrizes, princípios e responsabilidades para proteger os ativos informacionais da Universidade Nova Horizonte, assegurando que o tratamento, o acesso, o armazenamento e a transmissão de dados ocorram de maneira segura, ética, legal e alinhada às melhores práticas de segurança da informação.

A PSI visa também promover uma cultura organizacional baseada em responsabilidade digital, prevenção de incidentes e mitigação de riscos, de modo a garantir a confidencialidade, integridade, disponibilidade e legalidade da informação no ambiente institucional.

1.2. Escopo

Esta política se aplica a todos os usuários da instituição — alunos, docentes, técnicos, estagiários, visitantes e parceiros — que tenham acesso aos recursos de tecnologia da informação e comunicação (TIC), abrangendo ambientes locais, servidores em nuvem, redes, sistemas, dispositivos e serviços digitais da universidade.

2. Princípios de Segurança

A Política de Segurança da Informação da Universidade Nova Horizonte é sustentada por princípios fundamentais que norteiam todas as ações relacionadas à proteção dos ativos informacionais institucionais. Esses princípios asseguram que a informação seja tratada com responsabilidade, controle e conformidade, garantindo sua confiabilidade e valor institucional.

2.1. Confidencialidade

A confidencialidade visa garantir que o acesso à informação seja restrito apenas a pessoas devidamente autorizadas, prevenindo a exposição não autorizada de dados sensíveis. Isso se aplica especialmente a:

- Dados pessoais de alunos, professores, servidores e terceiros;
- Registros acadêmicos, financeiros e administrativos;
- Informações de pesquisa científica, projetos estratégicos e contratos institucionais.

Devem ser implementados mecanismos de controle de acesso, criptografia, classificação da informação e políticas de sigilo para preservar esse princípio em ambientes físicos e digitais.

2.2. Integridade

A integridade assegura que as informações mantidas, processadas ou transmitidas permaneçam íntegras, completas, coerentes e não adulteradas, protegendo-as contra modificações não autorizadas, falhas acidentais ou danos intencionais.

Esse princípio aplica-se a bancos de dados, sistemas de gestão acadêmica, documentos oficiais e registros institucionais. A rastreabilidade, a verificação de integridade (checksums, assinaturas digitais) e os logs de auditoria são práticas fundamentais para garantir sua preservação.

2.3. Disponibilidade

A disponibilidade garante que os recursos de tecnologia da informação, sistemas, dados e serviços estejam acessíveis e operacionais sempre que necessário, assegurando a continuidade das atividades acadêmicas, administrativas e de pesquisa, mesmo diante de falhas, incidentes ou desastres.

Este princípio requer a implementação de:

- Planos de continuidade e recuperação;
- Redundância de infraestrutura crítica;
- Monitoramento e resposta a falhas de sistema;
- Políticas de backup, manutenção preventiva e SLA (acordo de nível de serviço).

2.4. Legalidade

O princípio da legalidade assegura que todas as atividades de tratamento da informação sejam conduzidas em estrita conformidade com as normas legais, regulatórias e contratuais vigentes, incluindo:

- Lei Geral de Proteção de Dados Pessoais (LGPD – Lei nº 13.709/2018);
- Marco Civil da Internet (Lei nº 12.965/2014);
- Leis educacionais e normativas do MEC;
- Lei de Acesso à Informação (Lei nº 12.527/2011).

A universidade compromete-se com a promoção de uma cultura de respeito à privacidade, à transparência e à ética no uso das informações, adotando mecanismos de governança e compliance para garantir o cumprimento da legislação aplicável.

3. Gerenciamento de Acesso

O gerenciamento de acesso aos ativos informacionais da Universidade Nova Horizonte visa assegurar que somente usuários autorizados possam acessar sistemas, dados, dispositivos e serviços institucionais, de forma compatível com suas funções e responsabilidades. Essa prática é essencial para a proteção da confidencialidade, integridade e disponibilidade das informações.

Todas as atividades de concessão, alteração e revogação de acessos devem seguir processos formalizados, rastreáveis e conforme esta Política de Segurança da Informação.

3.1. Controle de Acesso

O controle de acesso será baseado no princípio do menor privilégio e da necessidade de saber, garantindo que cada usuário tenha apenas as permissões estritamente necessárias para o desempenho de suas funções.

- Toda conta de acesso será individual, nominal, única e intransferível, sendo a senha e os registros de acesso considerados equivalentes à assinatura pessoal do usuário.
- O uso dos ativos de informação deve estar alinhado às finalidades acadêmicas, administrativas, científicas e institucionais da universidade, vedado o uso indevido, pessoal ou ilícito. As contas deverão ser desativadas imediatamente em caso de desligamento, mudança de função ou encerramento de vínculo com a instituição.

- O sistema de controle de acesso deve registrar logs de autenticação, tentativas de login, trocas de senha e eventos suspeitos.

A delegação de acesso administrativo ou privilegiado exige aprovação formal e deve ser revista regularmente.

3.2. Autenticação

Todos os usuários devem ser autenticados em sistemas da Universidade por meio de credenciais válidas e seguras, compostas por:

- Nome de usuário (login institucional);
- Senha forte, com renovação periódica;
- Recomendação de autenticação multifator (MFA) obrigatória para sistemas críticos ou que contenham dados sensíveis, como servidores, sistemas acadêmicos, acesso remoto e ambiente em nuvem (ex: EC2 da AWS).

As senhas deverão obedecer aos seguintes critérios mínimos:

- Mínimo de 8 caracteres;
- Utilização de letras maiúsculas, minúsculas, números e caracteres especiais;
- Proibição de senhas reutilizadas ou de fácil adivinhação (ex: "123456", "admin", nome do usuário);
- Bloqueio automático após múltiplas tentativas incorretas de login.

3.3. Autorização

A autorização de acesso será baseada em grupos funcionais, perfis de cargo e segmentação organizacional (como departamentos e campi), com aplicação de:

- Segregação de funções (SoD), evitando conflitos de interesse e acessos excessivos;
- Políticas de acesso baseadas em papéis (RBAC - Role-Based Access Control);
- Revisões periódicas de permissões para garantir que os acessos continuem compatíveis com as funções exercidas;
- Registros e trilhas de auditoria para todas as alterações de privilégio, inclusive para usuários administradores.

Nenhum usuário poderá autoconceder permissões elevadas, e os acessos temporários ou emergenciais deverão ser controlados, justificados e documentados.

4. Segurança Física e Ambiental

A proteção dos ativos tecnológicos da Universidade Nova Horizonte vai além dos controles digitais: ela começa no espaço físico onde esses ativos estão instalados. A segurança física e ambiental visa preservar a integridade, a confidencialidade e a disponibilidade dos equipamentos, sistemas e informações contra acessos não autorizados, danos acidentais, sabotagens ou eventos naturais.

4.1. Proteção de instalações

Todos os ambientes que hospedam servidores, roteadores, switches centrais, equipamentos de backup e ativos críticos de rede devem ser instalados em áreas restritas, seguras e monitoradas. Essas áreas devem contar com:

- Portas com travamento eletrônico, de preferência com autenticação biométrica, cartão magnético ou PIN individual;
- Controle de acesso eletrônico com registro de entrada e saída (logs de acesso mantidos por no mínimo 12 meses);
- Sistema de videomonitoramento (CFTV) 24x7, com câmeras em pontos estratégicos, inclusive áreas de rack;
- Sinalização adequada de área restrita, proibindo acesso não autorizado e orientando sobre condutas em emergências.

O acesso às salas de equipamentos será concedido apenas a profissionais formalmente autorizados, com identificação visível e acesso individual intransferível. Terceiros (prestadores, técnicos externos) somente poderão entrar acompanhados por um responsável institucional, com registro formal de visita.

4.2. Controle de acesso físico

A universidade implementará políticas rigorosas de controle de acesso físico às áreas classificadas como sensíveis, incluindo:

- Credenciais personalizadas (crachás, tags ou cartões RFID) com controle de horário e setor de acesso permitido;
- Barreiras físicas (portas automatizadas, catracas, fechaduras magnéticas) nos pontos de entrada/saída das áreas técnicas;
- Revisão periódica da lista de pessoas autorizadas, com revogação imediata em caso de desligamento ou mudança de função;
- Auditoria rotineira dos registros de acesso, com verificação de acessos anômalos ou fora do expediente.

Toda tentativa de violação, acesso forçado ou falha de autenticação deverá ser registrada e tratada como incidente de segurança.

4.3. Segurança ambiental

Ambientes que abrigam infraestrutura de TI devem ser protegidos contra riscos ambientais, operacionais e acidentais. As medidas incluem:

- Climatização controlada (temperatura e umidade) com sensores e alarmes, para evitar superaquecimento e condensação;
- Sistemas de detecção e combate a incêndios com detectores de fumaça e extinção por gás inerte (como FM-200), compatível com equipamentos eletrônicos;
- Energia elétrica estabilizada com uso de nobreaks (UPS) de dupla conversão e geradores automáticos de emergência;
- Proteção contra surtos elétricos e descargas atmosféricas (SPDA e aterramento técnico); Sistema de alarme contra intrusão e presença de fumaça, com monitoramento remoto em tempo real;
- Política de manutenção preventiva, inspeções periódicas e testes de carga em equipamentos críticos.

Além disso, a universidade manterá um Plano de Recuperação de Desastres (DRP) para reagir a eventos catastróficos como incêndios, enchentes ou falhas estruturais graves, com orientações claras para continuidade dos serviços essenciais.

5. Segurança de Redes e Comunicações

A infraestrutura de rede da Universidade Nova Horizonte é responsável por suportar os serviços acadêmicos, administrativos e de pesquisa em ambientes locais e em nuvem. A segurança das comunicações — internas e externas — é essencial para garantir a integridade das operações, o sigilo das informações e a continuidade dos serviços críticos.

A instituição adota uma abordagem de defesa em profundidade, que combina tecnologias, processos e políticas de controle de tráfego, acesso e monitoramento ativo dos ambientes conectados.

5.1. Proteção de redes

A proteção das redes da universidade será realizada por meio de camadas de controle técnico e lógico, incluindo:

- Firewall de perímetro e segmentado: Controle do tráfego entre redes internas (por exemplo, administrativo, acadêmico, laboratorial) e entre redes internas e externas (internet, nuvem);
- Listas de controle de acesso (ACLs) e VLANs para segmentação de tráfego e isolamento de setores sensíveis;
- Configuração segura de roteadores e switches com autenticação, logs e restrição de comandos privilegiados;

- Criptografia de ponta a ponta (VPN/IPSec) para conexões externas autorizadas;
- Segurança em redes sem fio (Wi-Fi) com autenticação WPA2/WPA3 empresarial, ocultação de SSID e controle de dispositivos autorizados;
- Bloqueios de portas e serviços desnecessários em hosts e roteadores.

A conexão à internet é monitorada, autenticada e vinculada à identidade digital de cada usuário, permitindo rastreabilidade e responsabilização de atividades.

5.2. Monitoramento e detecção de intrusões

A universidade manterá mecanismos de monitoramento contínuo e detecção de atividades anômalas, com os seguintes recursos:

- Soluções de IDS (Intrusion Detection System) e IPS (Intrusion Prevention System), capazes de detectar e reagir a varreduras de rede, acessos indevidos, tentativas de exploração e comportamentos anômalos;
- Serviços de syslog centralizado e SIEM (Security Information and Event Management) para correlação de eventos, análise de padrões e resposta coordenada;
- Monitoramento de disponibilidade (uptime), latência e uso de banda com alertas em tempo real para gargalos ou quedas críticas;
- Auditoria periódica de logs e eventos de rede, com retenção mínima de 6 meses.

Em caso de detecção de intrusão, a resposta seguirá os procedimentos definidos no Plano de Gestão de Incidentes (ver item 6), priorizando a contenção, análise e recuperação dos serviços afetados.

O uso de ferramentas de análise de tráfego, sniffers, proxies ou qualquer tentativa de escaneamento de rede por usuários não autorizados constitui violação grave desta política e estará sujeito às penalidades administrativas e legais cabíveis.

6. Gestão de Incidentes de Segurança

A Universidade Nova Horizonte reconhece que incidentes de segurança da informação — como acessos não autorizados, vazamentos de dados, ataques cibernéticos, falhas operacionais ou indisponibilidades críticas — podem comprometer a integridade, a confidencialidade e a disponibilidade de seus ativos tecnológicos.

Para prevenir, detectar, responder e recuperar de tais eventos, a instituição manterá um Plano de Gestão de Incidentes de Segurança da Informação (PGISI), formalmente documentado, integrado ao plano de continuidade institucional, com os seguintes objetivos:

- Minimizar os impactos operacionais, acadêmicos, financeiros e reputacionais causados por falhas ou ataques;
- Restabelecer rapidamente os serviços afetados com segurança e controle;
- Preservar evidências técnicas para investigação forense, quando necessário;
- Promover o aprendizado organizacional com base nas causas-raiz dos eventos ocorridos.

6.1. Resposta a incidentes

Será estabelecido um processo estruturado de resposta a incidentes, composto pelas seguintes fases:

- Detecção e registro: Identificação do incidente por meio de logs, alertas de sistema, relatos de usuários ou ferramentas de segurança (IDS, antivírus, firewall);
Classificação e priorização: Avaliação da gravidade, abrangência e impacto do incidente, definindo o nível de resposta necessário;
- Contenção: Adoção imediata de ações para limitar a propagação ou o agravamento do problema;
- Erradicação e recuperação: Eliminação da causa-raiz e restauração segura dos sistemas afetados;

- Pós-incidente: Documentação do ocorrido, análise crítica, lições aprendidas e atualizações no plano de resposta.

O tempo de resposta será definido conforme a criticidade do sistema afetado, com prioridade máxima para serviços essenciais (como AD, DNS, Web, FTP, DHCP, e sistemas acadêmicos).

Um time de resposta a incidentes (TRI) será formalmente designado pela área de TI e composto por profissionais capacitados, com plano de escalonamento e contatos de contingência.

6.2. Relatórios de incidentes

Todos os membros da comunidade universitária (alunos, docentes, técnicos e terceiros) têm a responsabilidade de relatar imediatamente qualquer incidente, suspeita ou comportamento anômalo à equipe de segurança da informação.

Os canais oficiais de reporte incluem:

- Sistema de chamados da TI;
- E-mail de segurança
- Comunicação direta com o gestor de TI local.

Cada incidente será documentado em um registro oficial de ocorrências, contendo:

- Data e hora;
- Origem e escopo;
- Sistemas ou usuários afetados;
Ações corretivas adotadas;
- Evidências técnicas (logs, capturas de tela, relatórios);
- Responsáveis e conclusão do caso.

Os relatórios subsidiarão auditorias internas, revisões de políticas, processos disciplinares e a elaboração de ações preventivas.

7. Conscientização e Treinamento em Segurança

A disseminação da cultura de segurança da informação é uma ação estratégica fundamental para mitigar riscos operacionais e fortalecer a postura institucional diante de ameaças cibernéticas, erros humanos e condutas inadequadas no uso de recursos tecnológicos. A Universidade Nova Horizonte, alinhada às diretrizes de boas práticas internacionais e ao seu compromisso com a excelência acadêmica e administrativa, estabelece os seguintes programas permanentes de capacitação:

7.1. Programa de conscientização

Será desenvolvido e mantido um programa contínuo de conscientização em segurança da informação, destinado a todos os públicos internos — docentes, discentes, técnicos administrativos, estagiários e colaboradores terceirizados — visando:

- Reforçar a importância da proteção dos ativos informacionais da instituição;
- Estimular o comportamento seguro no uso de redes, sistemas e dispositivos;
- Minimizar incidentes causados por negligência, desconhecimento ou descuido;
- Apoiar o cumprimento da legislação vigente, especialmente a LGPD.

Como parte deste programa, a universidade disponibiliza uma Cartilha de Segurança da Informação com linguagem acessível, conteúdo visual e abordagem prática, distribuída em formato digital e físico. A cartilha aborda temas como: criação de senhas fortes, uso seguro de e-mails e redes sociais, cuidados com dispositivos móveis, engenharia social, boas práticas em ambientes de trabalho, políticas institucionais e canais de denúncia.

A cartilha é atualizada anualmente ou sempre que houver mudanças significativas nos riscos, ou nas políticas de segurança.

7.2. Treinamento em segurança

A universidade promoverá treinamentos periódicos obrigatórios em segurança da informação, adaptados aos diferentes perfis de usuários e níveis de acesso aos sistemas institucionais. Os treinamentos poderão ocorrer na modalidade presencial, online ou híbrida, e contemplarão:

- Boas práticas para proteção de dados e informações;
- Normas internas e obrigações do usuário;
- Reconhecimento de ameaças (phishing, malware, engenharia social etc.);
- Uso seguro de senhas, dispositivos, redes e sistemas acadêmicos;
- Procedimentos em caso de incidentes.

Para os colaboradores da área de TI, será exigido um nível avançado de capacitação, incluindo tópicos como criptografia, gestão de vulnerabilidades, resposta a incidentes e conformidade com a ISO/IEC 27001.

A participação nos treinamentos será registrada e monitorada pela equipe de TI, sendo condição obrigatória para manutenção de acessos privilegiados. A ausência injustificada poderá resultar em advertência formal ou suspensão temporária do acesso a sistemas institucionais, conforme diretrizes internas.

8. Avaliação e Melhoria Contínua

A manutenção da eficácia da Política de Segurança da Informação (PSI) exige um ciclo constante de avaliação, retroalimentação e aprimoramento. Para isso, a Universidade Nova Horizonte adota práticas sistemáticas de monitoramento, análise de desempenho, revisão documental e auditorias, de forma a garantir que os controles de segurança permaneçam atualizados, eficazes e aderentes às exigências legais, tecnológicas e institucionais.

8.1. Auditorias de segurança

Auditorias internas de segurança da informação e testes técnicos de vulnerabilidade (como scans de rede, análise de portas, testes de penetração autorizados) serão realizados semestralmente ou sempre que houver alterações significativas na infraestrutura tecnológica, como:

- Implementação de novos serviços ou sistemas;
- Integração de tecnologias em nuvem;
- Ampliação do escopo de dados sensíveis.

As auditorias devem verificar:

- A conformidade dos processos com a PSI;
- O cumprimento de obrigações legais (como a LGPD);
- A aplicação das políticas de controle de acesso e backup;
- A eficácia dos controles físicos e lógicos de segurança.

Todos os achados deverão ser registrados em relatório próprio, com plano de ação para correção de falhas e mitigação de riscos identificados.

8.2. Revisão de políticas e procedimentos

A Política de Segurança da Informação e seus procedimentos associados deverão ser revisados:

- No mínimo, uma vez ao ano (ciclo anual de revisão);
- Sempre que houver mudanças relevantes na legislação, infraestrutura tecnológica, modelo de governança ou ambiente de ameaças cibernéticas.

A revisão será coordenada pela equipe de segurança da informação, com participação de representantes da gestão acadêmica e administrativa. Toda nova versão será disponibilizada nos canais institucionais e comunicada aos usuários afetados.

8.3. Análise de riscos

A análise de riscos será conduzida de forma proativa e contínua, utilizando metodologias reconhecidas (como ISO 27005 ou matriz de risco qualitativa), visando:

- Identificar vulnerabilidades em ativos críticos;
- Avaliar impactos e probabilidades de incidentes;
- Priorizar medidas preventivas e planos de contingência.

A análise de riscos é obrigatória em projetos de implantação de novos sistemas, serviços ou integrações em nuvem, devendo constar como etapa formal no ciclo de desenvolvimento e implantação de soluções tecnológicas da universidade.

8.4. Medição de desempenho

A eficácia das ações de segurança será acompanhada por indicadores de desempenho (KPIs) definidos pela equipe de TI e revistos periodicamente. Entre os principais indicadores recomendados, destacam-se:

- Tempo médio de resposta a incidentes (MTTR);
- Número de falhas ou vulnerabilidades detectadas por ciclo de auditoria;
- Disponibilidade (uptime) dos servidores críticos (%);
- Índice de participação nos treinamentos obrigatórios (%);
- Tempo médio para aplicação de atualizações críticas (patches);
- Taxa de conformidade com controles de acesso e backup.

Os resultados serão apresentados em relatórios técnicos à direção da universidade, com propostas de melhorias baseadas em evidências e metas definidas para os ciclos seguintes.

9. Conformidade Legal e Regulatória

A conformidade com leis, normas e diretrizes regulatórias é um pilar essencial da governança em segurança da informação. A Universidade Nova Horizonte se compromete a adotar práticas que assegurem o uso ético, legal e responsável das informações institucionais, protegendo dados pessoais, corporativos e acadêmicos, e promovendo transparência, rastreabilidade e responsabilidade institucional.

9.1. Conformidade com leis e regulamentações

As políticas, normas operacionais e práticas de segurança da informação da Universidade Nova Horizonte estarão em estrita conformidade com a legislação nacional e com diretrizes específicas do setor educacional. Entre os principais marcos legais e normativos observados, destacam-se:

- Lei nº 13.709/2018 – LGPD (Lei Geral de Proteção de Dados Pessoais), que rege o tratamento de dados pessoais por pessoas jurídicas de direito público e privado;
- Lei nº 12.965/2014 – Marco Civil da Internet, que estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil;
- Normas e Portarias do Ministério da Educação (MEC), que regulam a oferta de cursos, registros acadêmicos e controle institucional;
- Lei de Acesso à Informação (Lei nº 12.527/2011), que estabelece regras de transparência e acesso a informações públicas;
- Normas ISO/IEC aplicáveis, como ISO/IEC 27001, 27002 e 27701 (para proteção de dados pessoais).

A equipe de Segurança da Informação atuará em conjunto com os setores Jurídico e Administrativo para garantir a aderência contínua às obrigações legais, auditorias regulatórias e recomendações de órgãos oficiais.

9.2. Gestão de Vulnerabilidades e Patches

Será mantido um processo estruturado e contínuo de identificação, avaliação e correção de vulnerabilidades técnicas, abrangendo toda a infraestrutura local e os ambientes hospedados em nuvem, com foco especial em:

- Sistemas operacionais (Windows Server, Ubuntu Server);
- Serviços de rede (Active Directory, DHCP, DNS, FTP, HTTP);
- Aplicações web e APIs institucionais;
- Instâncias e serviços na AWS (como EC2, S3, RDS).

As atualizações de segurança (patches) serão validadas, priorizadas e aplicadas conforme sua criticidade, utilizando ferramentas de automação sempre que possível, de modo a reduzir riscos operacionais e aumentar a eficácia da mitigação.

9.3 Atualizações de segurança

Todos os ativos computacionais da Universidade Nova Horizonte — incluindo servidores, estações, notebooks, dispositivos móveis, roteadores e serviços virtuais — devem ser mantidos atualizados com versões estáveis, seguras e homologadas. Para isso:

- A equipe de TI será responsável por monitorar alertas de segurança emitidos pelos fornecedores, fabricantes e comunidades técnicas;
- As atualizações serão validadas previamente em ambientes de homologação, quando disponíveis, para evitar incompatibilidades;
- A aplicação de patches será realizada preferencialmente em janelas de manutenção previamente agendadas, com comunicação aos setores impactados;
- Será mantido um registro formal das atualizações aplicadas, contendo datas, sistemas afetados, tipo de atualização, responsáveis e eventuais incidentes derivados;
- Sempre que tecnicamente viável, serão utilizadas ferramentas de gerenciamento centralizado de atualizações e scripts de automação.

A negligência na atualização de sistemas representa um risco direto à confidencialidade, integridade e disponibilidade das informações da instituição. Situações de omissão ou descumprimento poderão ser tratadas como falhas administrativas graves, sujeitas às sanções cabíveis.

10. Responsabilidades

A eficácia da Política de Segurança da Informação depende diretamente do engajamento, da clareza de papéis e da responsabilidade compartilhada entre todos os integrantes da comunidade universitária. A Universidade Nova Horizonte adota um modelo de governança colaborativa, em que todos — da alta direção aos usuários finais — têm obrigações definidas quanto à proteção dos ativos informacionais e à conformidade com esta política.

10.1. Direção Geral e Reitoria

- Estabelecer diretrizes estratégicas que assegurem a governança em segurança da informação;
- Garantir o alinhamento institucional entre a PSI e os objetivos acadêmicos e administrativos da universidade;
- Designar formalmente os responsáveis pela gestão da segurança da informação;
- Alocar recursos humanos, financeiros e tecnológicos necessários à implantação dos controles previstos nesta política;
- Estimular a cultura de segurança entre os gestores, colaboradores, professores e alunos, promovendo ações educativas, comunicados e campanhas institucionais.

10.2. Equipe de TI

- Planejar, implantar, operar e monitorar os controles de segurança lógicos, físicos e de rede descritos nesta política;
- Identificar vulnerabilidades, avaliar riscos e conduzir ações corretivas ou mitigatórias em caso de incidentes;
- Gerenciar backups, atualizações de sistemas, controle de acessos, criptografia e logs;
- Registrar, investigar e responder formalmente a incidentes de segurança da informação;
- Manter registros auditáveis das ações técnicas realizadas;
- Atuar como ponto focal para auditorias, inspeções ou diligências relacionadas à segurança da informação.

10.3. Gestores de Área

- Zelar pelo cumprimento da PSI em suas respectivas áreas;
- Garantir que os membros da sua equipe conheçam suas responsabilidades e sejam treinados adequadamente;
- Atuar de forma proativa na prevenção de incidentes e no estímulo às boas práticas no uso de sistemas e dados;
- Comunicar à TI eventuais não conformidades, comportamentos suspeitos ou necessidade de ajustes nas permissões de acesso;
- Apoiar a execução de auditorias, revisões de acesso e ações de melhoria contínua dentro da sua unidade organizacional.

10.4. Usuários

- Utilizar os recursos de tecnologia da informação e comunicação (TIC) da universidade de forma ética, segura, legal e responsável;
- Proteger credenciais de acesso, não compartilhando senhas ou dispositivos com terceiros;
- Reportar imediatamente qualquer incidente, falha ou comportamento suspeito que possa comprometer a segurança das informações;
- Manter-se atualizado quanto às diretrizes da PSI e participar obrigatoriamente dos treinamentos oferecidos;
- Cumprir os termos de uso dos sistemas institucionais e respeitar a privacidade, confidencialidade e integridade das informações acessadas.

Esta Política de Segurança da Informação representa um compromisso institucional com a proteção dos ativos da Universidade Nova Horizonte. Sua eficácia depende do envolvimento consciente e ativo de todos os colaboradores, professores, alunos e parceiros. Ao seguir estas diretrizes, contribuímos para um ambiente acadêmico mais seguro, confiável e preparado para os desafios do mundo digital.

10.4. Penalidades

Atos ou ações que violem o disposto nesta Resolução ou em quaisquer de suas normas e/ou procedimentos complementares, ou que prejudiquem os controles de segurança da informação, no âmbito da Universidade, serão apuradas mediante instauração de processo administrativo disciplinar e os responsáveis por prejuízos ou irregularidades responderão administrativa, civil e/ou penalmente pelos seus atos.

11. Glossário

A

Acesso não autorizado – Uso ou tentativa de uso de um recurso (sistema, rede ou dado) sem permissão expressa.

Administração de sistemas – Conjunto de tarefas realizadas para garantir a operação segura, estável e eficiente de sistemas de TI.

Análise de risco – Processo sistemático de identificação, avaliação e priorização de riscos associados a ativos informacionais.

Autenticação – Verificação da identidade de um usuário, sistema ou dispositivo (ex.: senhas, biometria, tokens).

Autorização – Processo de concessão de permissões de acesso a usuários após sua autenticação.

B

Backup – Cópia de dados mantida separadamente para permitir recuperação em caso de falha, perda ou desastre.

Base legal (LGPD) – Fundamento jurídico que autoriza o tratamento de dados pessoais segundo a Lei Geral de Proteção de Dados.

BYOD (Bring Your Own Device) – Política que permite que funcionários ou alunos utilizem seus dispositivos pessoais para acessar os sistemas institucionais.

C

CFTV (Circuito Fechado de Televisão) – Sistema de videomonitoramento utilizado para segurança de ambientes físicos.

Compliance – Conformidade com leis, normas e políticas internas.

Confidencialidade – Garantia de que a informação seja acessada apenas por pessoas autorizadas.

Criptografia – Técnica que transforma dados em formatos ilegíveis, acessíveis apenas mediante chave de decodificação válida.

Controle de acesso – Conjunto de medidas que restringem o acesso a sistemas, dados ou locais apenas a usuários autorizados.

D

Dados pessoais – Qualquer informação relacionada a pessoa natural identificada ou identificável.

Dados sensíveis – Categoria especial de dados pessoais que merecem proteção reforçada, como dados de saúde, religião, política etc.

Disponibilidade – Capacidade de acesso e uso de sistemas e informações sempre que necessário.

Dispositivo móvel – Equipamentos portáteis como smartphones, tablets ou notebooks com acesso à rede.

DRP (Disaster Recovery Plan) – Plano de recuperação de desastres que garante o restabelecimento dos serviços após eventos críticos.

E

Endpoint – Qualquer dispositivo final que se conecta à rede, como computadores, notebooks ou celulares.

Engenharia social – Técnica de manipulação psicológica para induzir pessoas a revelar informações confidenciais.

Exfiltração de dados – Transferência não autorizada de dados para fora da organização.

Escalabilidade – Capacidade de um sistema de crescer em desempenho ou tamanho conforme a demanda aumenta.

F

Firewall – Sistema de segurança que filtra o tráfego de entrada e saída em redes de computadores.

Forense digital – Análise técnica para identificar, preservar e investigar evidências digitais após incidentes.

G

Governança de TI – Conjunto de práticas que asseguram o alinhamento da tecnologia da informação com os objetivos da instituição.

Gestão de vulnerabilidades – Processo contínuo de identificação, análise e correção de falhas de segurança.

I

Identidade digital – Conjunto de informações usadas para identificar um indivíduo nos sistemas da universidade.

Incidente de segurança – Evento que compromete a confidencialidade, integridade ou disponibilidade da informação.

Integridade – Garantia de que os dados não foram alterados indevidamente, mantendo sua precisão e confiabilidade.

IPS/IDS – Sistemas de prevenção e detecção de intrusão, respectivamente, que monitoram atividades maliciosas na rede.

L

LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018), que regula o uso de dados pessoais no Brasil.

Logs – Registros automáticos de eventos, acessos ou ações realizadas em sistemas, essenciais para auditoria e investigação.

M

Malware – Software malicioso projetado para causar danos, roubo de dados ou interrupções (ex: vírus, trojans, ransomwares).

MFA (Autenticação Multifator) – Recurso de segurança que exige duas ou mais formas de verificação para autenticação.

Monitoramento contínuo – Supervisão constante dos sistemas e redes com o objetivo de identificar riscos ou falhas rapidamente.

P

PenTest (Teste de Penetração) – Simulação autorizada de ataques para testar a resistência de sistemas de segurança.

Phishing – Fraude que tenta enganar o usuário para obter informações sensíveis por meio de e-mails ou sites falsos.

Plano de continuidade de negócios (PCN) – Conjunto de medidas para garantir o funcionamento da instituição mesmo em situações críticas.

Política de Senhas – Regras que definem o padrão mínimo para criação, uso e renovação de senhas.

Privacidade – Direito do titular de dados de ter suas informações protegidas e utilizadas de forma ética e legal.

R

RBAC (Role-Based Access Control) – Modelo de controle de acesso baseado em funções e responsabilidades dos usuários.

Ransomware – Tipo de malware que bloqueia os dados e exige resgate para restaurá-los.

Redundância – Recurso que garante continuidade de serviço mesmo se um componente falhar.

Risco – Probabilidade de que uma ameaça explore uma vulnerabilidade, gerando impacto negativo.

S

Segurança da informação – Conjunto de práticas que garantem a confidencialidade, integridade e disponibilidade da informação.

Segregação de funções (SoD) – Prática que separa responsabilidades críticas para evitar conflitos de interesse.

SIEM (Security Information and Event Management) – Solução que coleta e analisa logs para identificar ameaças e gerar alertas de segurança.

Spoofing – Técnica usada por cibercriminosos para se passarem por entidades confiáveis.

T

TIC (Tecnologia da Informação e Comunicação) – Conjunto de recursos tecnológicos usados para gerar, armazenar, processar e transmitir informações.

Token – Dispositivo ou aplicação usada como segundo fator de autenticação.

TRI (Time de Resposta a Incidentes) – Equipe designada para detectar, conter e resolver eventos de segurança.

U

Uptime – Tempo em que um sistema ou serviço permanece disponível e funcionando corretamente.

Usuário privilegiado – Pessoa com acesso elevado a sistemas e dados sensíveis (ex.: administradores de sistemas).

V

VPN (Virtual Private Network) – Rede privada virtual que protege o tráfego de dados via criptografia em conexões públicas.

Vulnerabilidade – Falha ou brecha de segurança que pode ser explorada para causar danos.

W

Wi-Fi – Tecnologia sem fio para conexão à internet ou rede local, sujeita a regras específicas de segurança (ex.: WPA2).

Whitelist – Lista de elementos permitidos (sites, IPs, dispositivos), usada como mecanismo de controle.