IMEI Instituto Mariano de Estudos e Inovação

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Aracaju, 2026

Sumário

Política de Segurança da Informação

Esta Política de Segurança da Informação (PSI) tem como objetivo primordial estabelecer diretrizes, normas e responsabilidades que visam proteger os ativos de informação do Instituto Mariano de Estudos e Inovação – IMEI contra ameaças, sejam elas intencionais ou acidentais. A implementação desta política é fundamental para assegurar a continuidade das operações acadêmicas e administrativas, minimizar riscos e garantir a conformidade com as regulamentações vigentes, que preza pela fidedignidade e segurança dos dados institucionais.

2. ESCOPO E ABRANGÊNCIA

As diretrizes aqui estabelecidas aplicam-se a todos os colaboradores (docentes e técnico- administrativos), discentes, prestadores de serviço e quaisquer outros indivíduos que tenham acesso aos sistemas e à infraestrutura de Tecnologia da Informação (TI) do Instituto Mariano de Estudos e Inovação – IMEI. A política abrange todos os sistemas, dados, equipamentos e instalações que compõem o ambiente tecnológico da instituição.

3. PRINCÍPIOS DA SEGURANÇA DA INFORMAÇÃO

A presente política é fundamentada nos quatro pilares essenciais da Segurança da Informação:

- **3.1 Confidencialidade:** Assegurar que o acesso à informação seja concedido exclusivamente a pessoas autorizadas. Isso protege dados sensíveis, como registros acadêmicos, informações financeiras de alunos e dados pessoais de colaboradores, contra acessos indevidos.
- **3.2 Integridade:** Garantir que a informação mantenha sua exatidão, confiabilidade e origem, não sofrendo alterações indevidas. A integridade é vital para a validade de históricos escolares, pautas, dados de pesquisa e registros administrativos.
- **3.3 Disponibilidade:** Certificar que a informação e os sistemas associados estejam acessíveis e operacionais sempre que requisitados por usuários autorizados. A disponibilidade de sistemas como o Portal do Aluno, o Ambiente Virtual de Aprendizagem (AVA) e os sistemas de gestão acadêmica é crucial para o bom

andamento das atividades da instituição.

- **3.4 Autenticidade:** Prover mecanismos que garantam a identidade do usuário que está criando, acessando ou modificando uma informação, permitindo a rastreabilidade das ações e a responsabilização por elas.

4. DIRETRIZES DE SEGURANÇA

4.1 Segurança Física e do Ambiente

A proteção dos equipamentos que armazenam e processam as informações institucionais é a primeira camada de defesa.

- **Acesso Restrito ao Datacenter:** O acesso ao Datacenter é estritamente controlado e restrito a profissionais do setor de TI. O ambiente é mantido trancado, e as chaves de acesso são gerenciadas pelo departamento de TI, com uma cópia de segurança sob a guarda da Diretoria.
- **Climatização e Manutenção:** O Datacenter é equipado com sistema de climatização para manter a temperatura e a umidade em níveis ideais para o funcionamento dos servidores. Manutenções preventivas no sistema de ar-condicionado são realizadas semestralmente.
- **Proteção Elétrica:** Todos os servidores, equipamentos de rede e firewalls estão conectados a sistemas de alimentação ininterrupta (UPS/Nobreak) de uso exclusivo, garantindo a continuidade das operações em caso de falha no fornecimento de energia e protegendo os equipamentos contra surtos elétricos. Os UPS são submetidos a manutenções periódicas a cada seis meses.
- **Manutenção e Limpeza:** A limpeza do Datacenter é realizada semanalmente, sempre com a supervisão de um membro da equipe de TI, para evitar danos acidentais aos equipamentos.
    - **Estrutura de Rede Segura:** Os racks de equipamentos de rede, mesmo os localizados em outros prédios, são mantidos trancados, com acesso controlado pelo setor de TI.

5. Segurança Lógica e de Redes

A segurança lógica visa proteger os dados e sistemas contra acessos não autorizados

e ataques cibernéticos.

- **Firewall:** A rede da instituição é protegida por um firewall robusto e constantemente atualizado, que monitora e filtra o tráfego de rede, bloqueando tentativas de acesso malicioso.
- **Software Antivírus:** Todos os computadores da instituição possuem software de antivírus licenciado e com atualizações automáticas, garantindo a proteção contra malwares, spyware e outras ameaças.
- **Segurança nas Estações de Trabalho:** Os computadores de uso administrativo são protegidos por senhas individuais, pessoais e intransferíveis. O perfil de administrador local é de uso exclusivo da equipe de TI.

6. Gestão de Acessos

- **Credenciais Individuais:** O acesso a todos os sistemas corporativos (acadêmico, financeiro, administrativo) é realizado por meio de credenciais (usuário e senha) únicas, pessoais e intransferíveis. O compartilhamento de senhas é estritamente proibido.
- **Acesso Discente:** O sistema acadêmico e o ambiente virtual de aprendizagem (AVA) disponibilizados aos alunos também seguem a política de acessos individuais, garantindo a segurança e o sigilo de suas informações acadêmicas.

7. Cópias de Segurança (Backup) e Recuperação de Dados

Para garantir a integridade e a disponibilidade das informações, a instituição mantém uma rigorosa política de backup.

- **Backup de Sistemas Críticos:** É realizado backup diário, completo e incremental, dos sistemas essenciais e de seus respectivos bancos de dados.
- **Backup de E-mails:** Cópias de segurança das caixas de e-mail corporativas são realizadas periodicamente para prevenir a perda de informações relevantes.
- **Redundância e Armazenamento:** Os dados críticos são mantidos em servidores web seguros, com redundância de dados replicada para um servidor local, localizado no Datacenter do campus, assegurando múltiplas camadas de proteção e agilidade na recuperação em caso de falhas.

8. Uso do E-mail Corporativo

O e-mail corporativo é uma ferramenta oficial de comunicação e deve ser utilizado de forma profissional e segura.

- **Finalidade:** O e-mail deve ser usado prioritariamente para fins institucionais, relacionados às atividades de ensino, pesquisa, extensão e administração.
- **Segurança:** É vedado o envio de informações confidenciais ou sensíveis por e-mail sem a devida criptografia ou proteção. Os usuários devem estar atentos a e-mails de *phishing* e não devem clicar em links ou baixar anexos de fontes suspeitas.
- **Responsabilidade:** O conteúdo das mensagens enviadas é de responsabilidade do remetente. É proibido o uso do e-mail corporativo para a disseminação de spam, correntes, material ofensivo ou ilegal.

9. RESPONSABILIDADES

- **Departamento de TI:** É responsável por implementar, gerenciar e monitorar os controles de segurança descritos nesta política.
- **Usuários (Colaboradores e Alunos):** São responsáveis por zelar pela segurança de suas credenciais de acesso, utilizar os recursos de TI de forma consciente e reportar qualquer incidente de segurança ao departamento de TI.
- **Gestores:** São responsáveis por garantir que suas equipes compreendam e cumpram as diretrizes desta política.

10. DISPOSIÇÕES GERAIS

O descumprimento das normas estabelecidas nesta Política de Segurança da Informação sujeitará o infrator às sanções disciplinares cabíveis, conforme o regimento interno do Instituto Mariano de Estudos e Inovação – IMEI e a legislação em vigor. Esta política é revisada anualmente ou sempre que se fizer necessário para se adequar a novas tecnologias, ameaças e regulamentações.