

**MINISTÉRIO DA EDUCAÇÃO  
INSTITUTO FEDERAL DO AMAZONAS  
DIRETORIA DE GESTÃO DE TECNOLOGIA DA INFORMAÇÃO (DGTI)**

**MINUTA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO**

**MANAUS/AM  
2025**

## **CAPÍTULO I DAS DISPOSIÇÕES PRELIMINARES**

Art. 1º Esta Política de Segurança da Informação estabelece diretrizes e práticas para garantir a confidencialidade, integridade e disponibilidade dos ativos do Instituto Federal do Amazonas (IFAM), mitigando riscos e ameaças em todo seu ambiente institucional.

Art. 2º Para os efeitos desta Política, aplicam-se as definições contidas no Anexo I.

Art. 3º Esta Política de Segurança da Informação aplica-se aos seguintes grupos do IFAM:

- I - funcionários, sejam servidores efetivos ou temporários, do IFAM;
- II - contratados e terceiros que trabalham para o IFAM;
- III - funcionários de parceiros; IV - estagiários; e V - discentes e visitantes.

## **CAPÍTULO II DOS OBJETIVOS**

Art. 4º A Política de Segurança da Informação tem como objetivo garantir a confidencialidade, disponibilidade e integridade dos ativos, dados e processos internos do IFAM por meio de boas práticas, regulamentações e normas, mitigando riscos à segurança da informação.

## **CAPÍTULO III DAS DIRETRIZES GERAIS**

Art. 5º As diretrizes gerais desta Política abrangem as seguintes áreas:

- I - Inventário de Ativos;
- II - Proteção de Dados;
- III - Configuração Segura;
- IV - Gestão de Acessos;
- V - Gestão de Vulnerabilidades;
- VI - Gestão de Registros;
- VII - Proteções de Correio Eletrônico e *Web*;
- VIII - Defesas Contra *Malware*;
- IX - *Backups*;
- X - Gestão de Rede;
- XI - Treinamento e Conscientização; e
- XII - Resposta a Incidentes.

## **Seção I**

### **Do Inventário de Ativos**

Art. 6º Será estabelecido e mantido um inventário de ativos do IFAM, sejam *hardware* ou *software*, que podem armazenar ou processar dados, com registro de informações precisas e detalhadas que possibilitem sua rastreabilidade.

Art. 7º Ativos, sejam *hardware* ou *software*, não autorizados em todo o ambiente do IFAM serão identificados e gerenciados periodicamente.

Art. 8º Será garantido que os *softwares* utilizados no ambiente do IFAM recebam suporte ativo de seus desenvolvedores.

## **Seção II**

### **Da Proteção de Dados**

Art. 9º Será estabelecido, mantido e revisado periodicamente um processo de gestão de dados que trate a sensibilidade dos dados, seu proprietário, manuseio, limites de retenção e requisitos de descarte.

Art. 10. Será estabelecido, mantido e revisado periodicamente um inventário de dados sensíveis.

Art. 11. O descarte de dados será realizado de forma segura, seja físico ou lógico, garantindo que não seja recuperável.

Art. 12. Será garantido o uso de criptografia em dispositivos de usuários que possuam dados sensíveis ou confidenciais, quando suportado.

Art. 13. Recomenda-se o uso de criptografia para dados em trânsito.

## **Seção III**

### **Da Configuração Segura**

Art. 14. Será estabelecido, mantido e revisado um processo de configuração segura de dispositivos de usuários, dispositivos não computacionais e *softwares*.

Art. 15. Será estabelecido, mantido e revisado um processo de configuração segura para dispositivos de rede.

Art. 16. Será implementado o bloqueio automático de sessões de usuários e ativos após certo período de inatividade.

Art. 17. Serão implementados e gerenciados sistemas de *firewall* nos servidores e *hosts* internos, caso seja suportado.

Art. 18. Serão implementados meios seguros de gerenciar os ativos e *softwares* do IFAM, como *SSH (Secure Shell)*, *HTTPS (Hypertext Transfer Protocol Secure)* e soluções similares.

Art. 19. Contas padrão de acesso nos ativos e *softwares* do IFAM, como *root*, administrador e outras da mesma categoria, serão gerenciadas.

#### **Seção IV**

##### **Da Gestão de Acessos**

Art. 20. Será estabelecido, mantido e revisado periodicamente um inventário de contas de usuários e administradores dos sistemas de informação do IFAM, contendo informações suficientes para identificação do usuário.

Art. 21. Contas inativas dos sistemas serão identificadas e desabilitadas dentro do período de 60 (sessenta) dias.

Art. 22. As senhas deverão seguir os seguintes padrões de robustez:

- I - mínimo de 8 (oito) caracteres;
- II - letras maiúsculas, minúsculas, números e caracteres especiais;
- III - frases e palavras impessoais; e
- IV - combinações de caracteres variados, evitando padrões previsíveis como dados pessoais, repetição de caracteres ou sequências numéricas.

Art. 23. Quando suportado, os sistemas devem garantir que as últimas 5 (cinco) senhas não sejam reutilizadas.

Art. 24. Quando suportado, os sistemas devem exigir *MFA (Multi-Factor Authentication)* para as seguintes situações:

- I - aplicações expostas externamente;
- II - acesso remoto à rede; e
- III - acesso administrativo.

#### **Seção V**

##### **Da Gestão de Vulnerabilidades**

Art. 25. Será definido e revisado periodicamente um processo de gestão de vulnerabilidades aos ativos do IFAM.

Art. 26. Será definido, mantido e revisado periodicamente um processo de remediação de vulnerabilidades de acordo com seus riscos.

Art. 27. Será realizada a gestão de *patches* dos sistemas operacionais dos ativos do IFAM de forma periódica.

Art. 28. Serão realizadas varreduras de vulnerabilidades automatizadas em ativos internos do IFAM de forma periódica.

## **Seção VI**

### **Da Gestão de Registros**

Art. 29. Será definido, implementado e revisado periodicamente um processo de gestão de *logs* para fins de auditoria, considerando questões como coleta, revisão e retenção de *logs*.

Art. 30. Será garantido o armazenamento seguro dos *logs* de auditoria.

## **Seção VII**

### **Das Proteções de Correio Eletrônico e Web**

Art. 31. Será garantido o uso de navegadores e mensageiros eletrônicos atualizados e com suporte ativo.

Art. 32. Serão implementados serviços de filtragem em todos os ativos suportados para bloqueio de acesso a *sites* potencialmente mal-intencionados ou desnecessários para a realização de funções institucionais.

## **Seção VIII**

### **Das Defesas Contra *Malware***

Art. 33. Serão implementadas e mantidas em infraestrutura tecnológica do IFAM, quando suportado, soluções *anti-malware* com suas assinaturas atualizadas.

Art. 34. A execução e reprodução automática para mídias removíveis serão desativadas.

Art. 35. Será realizada a varredura automática de *malware* em mídias removíveis.

## **Seção IX**

### **Dos *Backups***

Art. 36. As diretrizes relacionadas à recuperação de dados estão dispostas na Política de *Backup* e Restauração de Dados Digitais do IFAM.

## **Seção X**

### **Da Gestão de Rede**

Art. 37. Será promovida a atualização constante da infraestrutura de rede, mantendo seus componentes atualizados.

Art. 38. Serão realizadas revisões periódicas das versões de *software* disponíveis.

## **Seção XI Do Treinamento e Conscientização**

Art. 39. Será definido e executado um programa de conscientização e treinamentos em segurança da informação dentro do IFAM, promovendo conhecimentos sobre engenharia social, práticas de autenticação, práticas de tratamento de dados e outros aspectos relevantes.

Art. 40. Serão realizadas revisões periódicas do conteúdo, adequando às necessidades atuais.

## **Seção XII Da Resposta a Incidentes**

Art. 41. Será definido um ou mais responsáveis para gerenciamento de incidentes internos, que deverá coordenar e documentar os esforços de resposta e recuperação a incidentes.

Art. 42. Serão realizadas revisões periódicas do gerenciamento de incidentes.

Art. 43. Serão definidas, mantidas e revisadas periodicamente as informações de contato para relatar incidentes de segurança.

Art. 44. Será estabelecido e revisado periodicamente um processo para relatar incidentes, sendo amplamente divulgado em todo IFAM. Este processo pode incluir cronograma de relatórios, pessoal para relatar, mecanismos para relatar e informações mínimas do incidente.

## **CAPÍTULO IV DAS COMPETÊNCIAS E RESPONSABILIDADES**

Art. 45. Caberá ao Comitê de Desenvolvimento Institucional assessorar o IFAM na consecução das diretrizes da Política de Segurança da Informação na reitoria e nos seus *campi*, bem como na avaliação e análise de assuntos relativos aos objetivos estabelecidos.

Art. 46. Caberá à Diretoria de Gestão de Tecnologia da Informação apoiar o desenvolvimento e revisão das políticas de segurança da informação e promover a cultura de segurança da informação no IFAM.

Art. 47. Caberá ao Setor de Tecnologia da Informação de cada *campus* garantir que as normas, procedimentos e orientações desta política sejam plenamente implementados e seguidos, trabalhando em conjunto com as demais áreas relacionadas.

Art. 48. Caberá à Equipe de Tratamento de Incidentes a responsabilidade em todo o processo de resposta a incidentes em segurança da informação.

Art. 49. Caberá aos usuários cumprir as normas, procedimentos e orientações descritas nesta política, garantindo a confidencialidade, integridade e disponibilidade das informações.

## **CAPÍTULO V DAS PENALIDADES**

Art. 50. Em caso de infração por parte dos grupos do Art. 3º listados nesta política, qualquer um que tomar conhecimento do ocorrido deverá informar imediatamente ao setor de gestão de tecnologia de sua unidade, e, no âmbito da Reitoria, à Diretoria de Gestão de Tecnologia da Informação.

Art. 51. O coordenador ou diretor de tecnologia da informação do respectivo *campus* irá avaliar e despachar junto ao Diretor-Geral do *campus*, que decidirá, podendo ser consultada a Diretoria de Gestão de Tecnologia da Informação do IFAM ou a Procuradoria Jurídica do IFAM, acerca do encaminhamento que deverá ser adotado, nos termos da Lei nº 8.112/1990, da Instrução Normativa nº 14, de 14 de novembro de 2018, da Organização Didática do IFAM, da legislação e normativos que venham a substituí-los e de dispositivos legais e normativos específicos.

## **CAPÍTULO VI DA ATUALIZAÇÃO**

Art. 52. Esta Política de Segurança da Informação deve ser revisada quando necessário ou no prazo de 2 (dois) anos.

## **CAPÍTULO VII DAS DISPOSIÇÕES FINAIS**

Art. 53. A implementação das diretrizes dispostas nesta política dependerá da disponibilidade de recursos financeiros, humanos e tecnológicos do IFAM.

Art. 54. Caso não seja possível contemplar todos os ativos, dados e processos que compõem a estrutura do IFAM nas ações planejadas desta política, deverão ser priorizados inicialmente os ativos críticos da instituição.

Art. 55. Os sistemas legados incapazes de receber atualizações de segurança ou implementar as ações previstas nesta política devem ser identificados, junto aos seus riscos, para que sejam tomadas providências de redução dos riscos.

Art. 56. O usuário é responsável pelas atividades geradas pelas suas credenciais e irá responder por qualquer ação indevida realizada por meio de seu acesso.

Art. 57. É estritamente proibido o compartilhamento de credenciais de acesso aos sistemas do IFAM.

## ANEXO I

### TERMOS E DEFINIÇÕES

- **ATIVO:** Recursos que possuem valor para uma organização e que devem ser protegidos.
- **ATIVO CRÍTICO:** Recursos essenciais para operacionalização das atividades institucionais.
- **AUTENTICAÇÃO:** Processo de verificar a identidade de um usuário ou sistema.
- **BACKUP:** Cópia de dados que é mantida para recuperação.
- **CONFIDENCIALIDADE:** Garantia de que a informação é acessível apenas para pessoas autorizadas.
- **CRIPTOGRAFIA:** Técnica de codificação de informações para proteger sua confidencialidade.
- **DADOS EM TRÂNSITO:** Dados ou informações que são transmitidas entre sistemas ou dispositivos em uma rede.
- **DISPONIBILIDADE:** Garantia de que as informações e sistemas estão acessíveis quando necessário.
- **DISPOSITIVOS NÃO COMPUTACIONAIS:** Dispositivos que não possuem capacidade de processamento ou execução de tarefas computacionais.
- **ENGENHARIA SOCIAL:** Conjunto de técnicas de manipulação que explora erros humanos para obter informações confidenciais e acessos não autorizados.
- **HARDWARE:** Componentes físicos de um sistema de computação.
- **HTTPS (Hypertext Transfer Protocol Secure):** Protocolo de comunicação seguro para transferência de dados na *web*.
- **INFORMAÇÃO:** Dados processados que têm significado e valor.
- **INTEGRIDADE:** Garantia de que a informação não foi alterada.
- **LOGS:** Registros de eventos ou atividades em um sistema.
- **MALWARE:** Códigos maliciosos projetados para causar danos a sistemas.
- **MFA (Multi-Factor Authentication):** Método de autenticação que exige mais de uma forma de verificação para conceder acesso.
- **PATCH:** Atualização ou correção de *software* que resolve falhas, melhora a segurança ou adiciona funcionalidades.
- **RISCO:** Combinação da probabilidade de ocorrência de um evento e de suas consequências.
- **SEGURANÇA DA INFORMAÇÃO:** Conjunto de práticas e medidas para proteger a informação.
- **SOFTWARE:** Conjunto de instruções e programas que permitem o computador executar tarefas específicas.
- **SSH (Secure Shell):** Protocolo que fornece uma maneira segura de acessar e gerenciar sistemas remotamente.