POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DO IF SUDESTE MG

CAPÍTULO I DISPOSIÇÕES GERAIS

Seção I
Dos objetivos

Art. 1º A Política de Segurança da Informação (POSIN) do Instituto Federal de Educação, Ciência e Tecnologia do Sudeste de Minas Gerais - IF Sudeste MG - é uma declaração formal do IF Sudeste MG acerca do seu compromisso com a proteção dos ativos de informação de sua propriedade e/ou sob sua guarda.

Art. 2º Esta POSIN estabelece diretrizes e responsabilidades adequadas para o manuseio, tratamento, controle e proteção dos ativos de informação pertinentes ao IF Sudeste MG, em conformidade com a legislação vigente, com os valores éticos e com as melhores práticas de segurança da informação.

Seção II
Da abrangência

Art. 3º Esta Política, suas normas complementares e procedimentos aplicam-se a todos os campi, unidades e entidades vinculadas ao IF Sudeste MG, devendo ser cumprida pelos seguintes grupos:

I – servidores;
II – docentes substitutos e voluntários;
III – comunidade discente;
IV – terceirizados;
V – estagiários;
VI – servidores aposentados; e
VII – qualquer um que tenha acesso aos ativos de informação do IF Sudeste MG.

Art. 4º Todos aqueles mencionados no artigo anterior são responsáveis pela proteção dos ativos de informação de propriedade ou custodiados pelo IF Sudeste MG, e devem estar comprometidos com o cumprimento desta política, normas e procedimentos complementares.

Seção III
Dos princípios

Art. 5º A Política de Segurança da Informação do IF Sudeste MG está fundamentada na preservação das informações necessárias às atividades da Instituição e terá como base os seguintes princípios:

I – Responsabilidade: os agentes públicos devem conhecer e respeitar a POSIN do IF Sudeste;
II – Ética: os direitos dos agentes públicos devem ser preservados, sem o comprometimento da segurança da informação;
III – Celeridade: às ações de segurança da informação devem oferecer respostas rápidas a incidentes e falhas de segurança;
IV – Clareza: as regras de segurança da informação devem ser precisas, concisas e de fácil entendimento;
V – Privacidade: informação que fira o respeito à intimidade e à honra dos cidadãos não pode ser divulgada;
VI – Publicidade: dar transparência no trato da informação, observados os critérios legais;
VII – Autenticidade: garantir a veracidade da autoria da informação;
VIII – Confidencialidade: garantir que somente pessoas devidamente autorizadas devem ter acesso à informação;
IX – Integridade: somente alterações, supressões e adições autorizadas devem ser realizadas nas informações;
X – Disponibilidade: a informação deve estar disponível para as pessoas autorizadas sempre que necessário ou demandado; e
XI – Legalidade: o uso da informação deve estar de acordo com as leis, regulamentos, licenças e contratos em vigência.

Parágrafo único: Serão observados ainda, sem prejuízo dos demais, outros princípios constitucionais que regem a Administração Pública Federal.

Seção IV
Dos Conceitos e Definições

Art. 6º Para os fins desta Resolução considera-se:

I – Ameaça: causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou para a Instituição;
II – Ativo: recursos que possuem valor para uma organização e que devem ser protegidos;
III – Ativo crítico: ativos fundamentais para a continuidade das operações;
IV – Ativos de informação: são todos os recursos e componentes utilizados na produção, armazenamento, transmissão e processamento da informação;
V – Autenticação: processo de verificar a identidade de um usuário ou sistema;

. VI – Backup: cópia de dados que é mantida para recuperação;

VII – Classificação da informação: atribuição, pela autoridade competente, de grau de sigilo, disponibilidade e integridade dado à informação, documento, material, área ou instalação;

VIII – Criptografia: técnica de codificação de informações para proteger sua confidencialidade;

IX – Dispositivos móveis: equipamentos portáteis dotados de capacidade computacional ou dispositivos removíveis de memória para armazenamento, entre os quais se incluem, não limitando a estes: notebooks, netbooks, smartphones, tablets, pendrives, USBdrives, HD externo, e cartões de memória;

X – Dispositivos não computacionais: dispositivos que não possuem capacidade de processamento ou execução de tarefas computacionais.

XI – Engenharia social: conjunto de técnicas de manipulação que explora erros humanos para obter informações confidenciais e acessos não autorizados;

XII – Gestor da informação: qualquer servidor ou unidade do IF Sudeste MG que, no exercício de suas competências é responsável pela produção, administração ou tratamento, ainda que temporário, de informações geridas nos processos de trabalho sob sua responsabilidade;

XIII – Hardware: componentes físicos de um sistema de computação;

XIV – Informação: dados processados que têm significado e valor;

XV – Logs: registros de eventos ou atividades em um sistema;

XVI – Malware: códigos maliciosos projetados para causar danos a sistemas;

XVII – Patch: Atualização ou correção de software que resolve falhas, melhora a segurança ou adiciona funcionalidades.

XVIII – Política de Mesa e Tela Limpa: conjunto de diretrizes que estabelece a obrigatoriedade de manter espaços de trabalho organizados e livres de documentos e informações sensíveis.

XIX – Risco: combinação da probabilidade de ocorrência de um evento e de suas consequências;

XX – Segregação de funções: modo de garantir que nenhuma ação individual poderá comprometer a segurança de um sistema ou obter acesso não autorizado aos dados;

XXI – Software: programa de computador desenvolvido para executar um conjunto de ações previamente definidas;

XXII – SSH: Secure Shell, protocolo que fornece uma maneira segura de acessar e gerenciar sistemas remotamente; e

XXIII – Conteúdo não autorizado: Conteúdo que pode representar ameaça à segurança cibernética dos ativos de informação institucionais ou legalmente vedado; ou aquele identificado por mecanismos automáticos de segurança ou pelos administradores de rede.

Parágrafo único. Os demais termos utilizados nesta POSIN observará, no que couber, os conceitos constantes do Glossário de Segurança da Informação aprovado pela Portaria GSI/PR nº 93, de 26 de setembro de 2019.

CAPÍTULO II
DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Art. 7º A POSIN do IF Sudeste MG é composta por um conjunto de documentos com três níveis hierárquicos independentes e harmônicos entre si, relacionados a seguir:

I – Política de Segurança da Informação (POSIN): constituída neste documento, define a estrutura, as diretrizes gerais e as obrigações referentes à Segurança da Informação do IF Sudeste MG;
II – Normas de Segurança da Informação (Normas): estabelecem obrigações e procedimentos definidos de acordo com as diretrizes gerais da POSIN, a serem seguidos em diversas instâncias em que a informação é tratada. A cada Norma será associado um conjunto de procedimentos técnicos destinados a orientar sua implementação; e
III – Procedimentos de Segurança da Informação (Procedimentos): instrumentalizam o disposto na Política e nas Normas, permitindo a direta aplicação nas atividades do IF Sudeste MG.

Parágrafo único: Esta POSIN considera que toda e qualquer informação gerada, adquirida, utilizada ou armazenada pelo IF Sudeste MG é patrimônio da instituição e deve ser protegida quanto aos aspectos de confidencialidade, autenticidade, integridade e disponibilidade.

CAPÍTULO III
DA ESTRUTURA PARA GESTÃO DA SEGURANÇA DA INFORMAÇÃO

Art. 8º A gestão da segurança da informação do IF Sudeste MG será estruturada por:

I – um gestor de Segurança da Informação;
II – o Comitê de Segurança da Informação e Comunicação;
III – o Conselho de Governança Digital (COGD); e
IV – uma Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticoss (ETIR).

Seção I

Da Autoridade Máxima do IF Sudeste MG

Art. 9º Compete à autoridade máxima do IF Sudeste MG:

I – fornecer os subsídios necessários para aplicação da POSIN;
II – prover a orientação e o apoio necessários às ações de Segurança da Informação (SI), de acordo com os objetivos estratégicos, com as leis e regulamentos pertinentes;
III – indicar e nomear, dentre o quadro de servidores efetivos do IF Sudeste MG, um servidor para ser o Gestor de Segurança da Informação; e
IV – instituir a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR).

Seção II

Do Gestor de Segurança da Informação

Art. 10º O gestor de segurança da informação será designado dentre os servidores do IF Sudeste MG ocupantes de cargo efetivo, com formação ou capacitação técnica compatível às suas atribuições.

Art. 11 Compete ao Gestor de Segurança da Informação:

I – Presidir e coordenar o Comitê de Segurança da Informação e Comunicação (CSIC);
II – coordenar a elaboração da Política de Segurança da Informação, das normas e procedimentos de segurança da informação;
III – promover a cultura de SI no Instituto;
IV – acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;
V – propor recursos necessários às ações de SI;
VI – acompanhar os trabalhos da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR), podendo atuar como agente responsável de acordo com o Regulamento de Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos – ETIR do IF Sudeste MG;
VII – realizar e acompanhar estudos de novas tecnologia, quanto a possíveis impactos na SI;
VIII – manter contato permanente com outros Órgãos e Entidades da Administração Pública Federal para o trato de assuntos relativos à SI; e
IX – deliberar sobre questões de segurança da informação assessorado pelo CSIC.

Seção III

Do Comitê de Segurança da Informação e Comunicação - CSIC

Art. 12 O CSIC será de caráter permanente e vinculado administrativamente ao Conselho de Governança Digital (COGD), possuindo natureza consultiva e propositiva nas políticas e ações em sua área de competência no âmbito do IF Sudeste MG.

Art. 13 São competências do Comitê de Segurança da Informação e Comunicação:

I – assessorar o Gestor de Segurança da Informação do IF Sudeste MG em suas atividades descritas no Art. 12, inclusive como instância consultiva;
II – participar da elaboração da Política de Segurança da Informação e suas revisões, bem como zelar pelo seu processo de implementação;
III – propor normas e procedimentos metodológicos para implementação da política de segurança da informação;
IV – recomendar procedimentos técnicos e operacionais no uso da Internet e da Intranet;
V – propor políticas de conscientização e treinamento dos usuários para o uso dos recursos e sobre o seu papel na segurança da informação;
VI – acompanhar as investigações e as avaliações dos danos decorrentes das violações de segurança da informação;
VII – avaliar a necessidade de implementação de novas tecnologias relacionadas às políticas de segurança da informação, assegurando seu alinhamento às prioridades e estratégias institucionais à disponibilidade orçamentária;
VIII – participar de grupos de trabalho para assessorar o Conselho de Governança Digital em assuntos específicos; e
IX – elaborar seu regulamento próprio e propostas de posteriores alterações, sempre submetendo-as à apreciação do Conselho de Governança Digital e, posteriormente, à aprovação do Conselho Superior.

Seção IV

Do Conselho de Governança Digital - COGD

Art. 14 É um órgão de natureza estratégica e caráter permanente que tem por finalidade deliberar sobre políticas, diretrizes e planos relativos à governança da Tecnologia da Informação e Comunicação no âmbito do IF Sudeste MG.

Art. 15 Nos aspectos relacionados à segurança da informação, o COGD terá a competência de apreciar e aprovar a Política de Segurança da Informação e suas revisões, normas complementares e procedimentos, bem como acompanhar seu processo de implementação.

Seção V

Da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos – ETIR

Art. 16 A Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR) terá como objetivo receber, analisar, monitorar, coordenar e propor respostas a notificações e atividades relacionadas a incidentes de segurança da informação e comunicações no âmbito do IF Sudeste MG.

Art. 17 A ETIR do IF Sudeste MG será estruturada pelos seguintes membros:

I – o gestor de segurança da informação indicado pela autoridade máxima do IF Sudeste MG;
II – um representante de cada campus indicado pelos seus respectivos Diretores Gerais;
III – o coordenador de Infraestrutura de Redes e Comunicação (CIRC).

Art. 18 Compete Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR):

I – receber, analisar e responder aos incidentes de segurança da informação envolvendo redes computacionais do IF Sudeste MG;
II – organizar e centralizar as atividades para o tratamento e resposta de incidentes cibernéticos do IF Sudeste MG;
III – manter registro dos incidentes cibernéticos notificados ou detectados, com o objetivo de assegurar registro histórico das atividades da ETIR;
IV – coletar evidências em caso de incidentes de segurança da informação na rede interna de computadores.
V – gerenciar ações de contingência em conjunto com setores técnicos da área de TI;
VI – colaborar de maneira mútua com outros grupos de resposta a incidentes externos à instituição;
VII – emitir relatórios e pareceres técnicos relativos à segurança cibernética; e
VIII – recomendar o aperfeiçoamento ou a implementação de novos controles de segurança da informação;

CAPÍTULO VI
DIRETRIZES GERAIS

Seção I

Tratamento e Classificação de Dados e Informações

Art. 19 Aspectos relacionados ao tratamento, classificação e retenção de dados estão dispostos na Política de Proteção de Dados do IF Sudeste MG.

Art. 20 O tratamento das informações pessoais deve considerar o respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais, conforme o disposto na Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados - LGPD), na Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação - LAI), normativos internos e legislações aplicáveis.

Art. 21 Todas as informações devem ser adequadamente armazenadas e protegidas quanto ao uso e acesso fazendo uso de controles de criptografia adequados quando suportado, conforme definido em sua classificação de segurança previstas na Lei nº 12.527/2011, normativos internos e legislações aplicáveis.

Art. 22 Quando suportado, o uso de criptografia deve ser utilizado para dados e informações em trânsito.

Seção II
Segurança Física e do Ambiente

Art. 23 A segurança física e patrimonial em relação à segurança da informação tem por objetivo prevenir danos e interferências nas instalações do IF Sudeste MG que possam causar perda, roubo ou comprometimento das informações.

Art. 24 Os ativos de informação do IF Sudeste MG devem ser protegidos contra acesso físico não autorizado, danos, perdas, furto e interferência.

Art. 25 Todo equipamento deverá ser protegido e colocado em local visando a redução de riscos de ameaças e perigos do meio ambiente, bem como das oportunidades de acesso não autorizado.

Art. 26 Os equipamentos de operação crítica como os alocados no Data Center Institucional e nos demais Data Centers das Unidades deverão ser protegidos por fontes de alimentação adequada visando garantir a proteção e a continuidade dos serviços após os casos de falha e/ou surtos elétricos.

Art. 27. Todo equipamento, informação ou software de propriedade do IF Sudeste MG será retirado de suas dependências apenas mediante autorização prévia.

Art. 28 Deverá ser estabelecido por procedimento específico o descarte seguro de mídias de armazenamento de dados, visando assegurar a remoção de dados sensíveis.

Art. 29 Devem ser previstos procedimentos que visem resguardar o acesso não autorizado a informações e dados pessoais que estejam em meio físico ou digital, adotando políticas de "mesa limpa/tela limpa" sempre que possível.

Seção III
Gestão de Incidentes em Segurança da Informação

Art. 30 Os incidentes de segurança deverão ser identificados, monitorados, comunicados e devidamente tratados de forma a impedir a interrupção das atividades e não afetar o alcance dos objetivos estratégicos do IF Sudeste MG.

Art. 31 Os agentes públicos e as partes externas que usam os sistemas e serviços de informação do IF Sudeste MG deverão ser instruídos a notificar e registrar quaisquer fragilidades de segurança da informação, observada ou suspeita, nos sistemas ou serviços.

Art. 32 Os eventos de segurança da informação deverão ser avaliados e decididos se a sua classificação será de incidente de segurança da informação pela ETIR.

Art. 33 Os conhecimentos obtidos da análise e resolução dos incidentes de segurança da informação deverão ser documentados e armazenados em uma base de conhecimento que poderá ser utilizada para reduzir a probabilidade ou o impacto de incidentes futuros.

Art. 34 Os procedimentos para a identificação, coleta, aquisição e apresentação das informações serão definidos e aplicados pela ETIR, sob a supervisão do Comitê de Segurança da Informação e Comunicação.

Seção IV
Gestão de Ativos

Art. 35 Os ativos de informação devem ser inventariados e protegidos, utilizando-os estritamente dentro do seu propósito, sendo vedado seu uso para fins particulares ou de terceiros, entretenimento, veiculação de opiniões político-partidárias, religiosas, discriminatórias e afins. O inventário de ativos de informação deve ser revisado dentro de período de 01 (um) ano.

Art. 36 Os ativos não autorizados devem ser identificados e tratados, de forma que limite o acesso ao ambiente do IF Sudeste MG e suas informações.

Art. 37 O usuário é responsável pelas atividades realizadas por seu dispositivo móvel, respondendo por qualquer violação desta POSIN decorrente deste uso.

Art. 38 Os ativos de informação como *softwares,* sistemas e aplicativos devem ser devidamente atualizados e possuir suporte ativo de seus desenvolvedores.

Art. 39 Os sistemas legados essenciais para a operação interna deverão ser identificados, encontrando meios de mitigar os riscos envolvidos.

Art. 40 Os ativos de infraestrutura de rede deverão manter-se atualizados, realizando revisões em um período de 01 (ano). Os ativos de infraestrutura considerados críticos deverão ser revisados semestralmente.

Art. 41 Todos os ativos de informação do IF Sudeste MG devem ter ao menos um servidor custodiador.

Art. 42 Após o fim do vínculo com a Instituição, o agente público deverá devolver todos os ativos de informação do IF Sudeste MG em sua posse.

Art. 43 O acesso e o uso da informação, bem como dos ativos de informação deverão ser utilizados de acordo com as atribuições necessárias para o cumprimento das atividades institucionais. Qualquer outra forma de uso necessitará de prévia autorização.

Seção V
Gestão do Uso dos Recursos Operacionais e de Comunicações

Uso de Dispositivo Móvel

Art. 44 A política para uso de dispositivos móveis deve considerar:

I – registros dos dispositivos móveis;
II – requisitos para a proteção física;
III – restrições quanto à instalação de software;
IV – requisitos para as versões dos *softwares* e aplicações de pacotes de segurança;
V – controle de acesso;
VI – técnicas criptográficas;
VII – proteção contra malware;
VIII – *backup*; e
IX – uso dos serviços e aplicações web.

Parágrafo único: Os usuários serão orientados sobre o correto uso dos dispositivos móveis por meio de campanhas de conscientização.

Correio Eletrônico

Art. 45 O correio eletrônico institucional é considerado uma forma de comunicação oficial e deve ser utilizado exclusivamente no desempenho das atividades institucionais.

Art. 46 A utilização do correio eletrônico institucional pelos usuários previstos no Art. 3º deve respeitar o regulamento de uso e administração do serviço de correio eletrônico institucional no âmbito do Instituto Federal de Educação, Ciência e Tecnologia do Sudeste de Minas Gerais.

Art. 47 Os mensageiros de correio eletrônico utilizados devem estar atualizados e com suporte ativo pelos seus desenvolvedores.

Art. 48 Os mensageiros de correio eletrônico deverão utilizar filtros *antispam*, impossibilitando também possíveis arquivos desnecessários no ambiente do IF Sudeste MG.

Acesso à Internet

Art. 49 O acesso à Internet, por meio da rede de dados do IF Sudeste MG, é uma concessão e deve ter seu uso orientado para a execução das atividades institucionais.

Art. 50 Os navegadores utilizados para acessar a internet devem estar atualizados e com suporte ativo pelos seus desenvolvedores.

Art. 51 O *download* de arquivos não autorizados e que não tenham relação com o cumprimento de atividades institucionais são estritamente proibidos.

Art. 53 O uso da internet poderá ser monitorado e registrado para fins de auditoria e segurança interna.

Computação em Nuvem

Art. 54 Sempre que houver a necessidade de considerar a adoção da computação em nuvem no IF Sudeste MG, será adotada, por meio de norma complementar, medidas que assegurem os pilares da segurança da informação, bem como o preconizado nas legislações e orientações normativas vigentes.

Art. 55 O contrato de prestação de serviço, quando for o caso, deverá conter cláusulas que garantam a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações hospedadas na nuvem, em especial aquelas sob custódia e gerenciamento do prestador de serviço.

Art. 56 Deverá ser desenvolvida uma estratégia de uso de software e de serviços de computação em nuvem no âmbito do Instituto Federal de Educação, Ciência e Tecnologia do Sudeste de Minas Gerais.

Seção VI
Segurança nas Operações

Art. 57 Controles apropriados devem ser implementados buscando separar os ambientes de desenvolvimento, teste e produção, visando reduzir os riscos de acessos ou modificações não autorizadas aos sistemas operacionais e aos dados do negócio. Os ambientes de desenvolvimento, teste e produção deverão ser separados para reduzir os riscos de acessos ou modificações ao ambiente de produção.

Art. 58 As aplicações desenvolvidas internamente deverão seguir práticas de desenvolvimento seguro, mitigando possíveis riscos atrelados à segurança da informação.

Art. 59 Os controles de detecção, prevenção, recuperação e proteção contra malware, devem ser combinados com um adequado programa de conscientização do usuário.

Art. 60 Softwares anti-*malware* deverão estar presentes em todos os ativos internos sempre que suportado.

Art. 61 As cópias de segurança das informações, dos softwares e das imagens do sistema devem ser efetuadas e testadas regularmente conforme os requisitos definidos na Norma de Backup e Restauração de Dados Digitais.

Art. 62 Os registros de eventos (log) das atividades dos usuários, exceções, falhas e eventos de segurança da informação devem ser produzidos, mantidos e analisados criticamente, a intervalos regulares.

Art. 63 As informações dos logs e os seus recursos devem ser protegidos contra acesso não autorizado e adulteração.

Art. 64 As atividades dos administradores e operadores dos sistemas deverão ser registradas, protegidas e analisadas criticamente, a intervalos regulares.

Art. 65 Os relógios de todos os sistemas de processamento de informações do IF Sudeste MG deverão ser sincronizados com uma fonte de tempo precisa, visando um maior controle e auditabilidade.

Art. 66 Deverão ser estabelecidos controles para instalação, atualização e remoção de software nos sistemas operacionais.

Art. 67 Os ativos do IF Sudeste MG que incluem dispositivos de usuário final, dispositivos não computacionais, servidores e *softwares* deverão estar contemplados em um processo de configuração segura. Este processo deve passar por revisões periódicas, adequando-se às novas necessidades.

Art. 68 Os dispositivos móveis que representem risco aos pilares da segurança da informação em todo o ambiente do IF Sudeste MG poderão ser bloqueados da rede interna.

Art. 69 Os ativos do IF Sudeste MG deverão implementar bloqueio de sessão após um período definido de inatividade nos ativos quando suportado.

Art. 70 Os ativos que podem ser gerenciados remotamente deverão utilizar meios seguros de comunicação como, por exemplo, o *Secure Shell* (SSH).

Art. 71 Deverá ser estabelecido um processo de gestão de vulnerabilidades para os ativos do IF Sudeste MG, considerando os seguintes aspectos:

I – Remediação das vulnerabilidades identificadas baseada em seus respectivos riscos;
II – Gestão automatizada de *patches* do sistema operacional;
III – Gestão automatizada de *patches* de aplicações; e
IV – Período de revisão do processo.

Seção VII
Segurança nas Comunicações

Art. 72 As redes de dados deverão ser gerenciadas e controladas visando a proteção das informações nos sistemas e aplicações.

Art. 73 Os servidores e dispositivos de usuários dos quais o IF Sudeste MG tem controle deverão, quando suportado, implementar e gerenciar soluções de *firewall* ou semelhantes, garantindo segurança no tráfego de informações.

Art. 74 Os mecanismos de segurança, níveis de serviços e requisitos de gerenciamento dos serviços de rede deverão ser identificados e incluídos em qualquer acordo de serviço de rede, tanto para serviços de rede providos internamente como para terceirizados.

Art. 75 Os grupos de serviços de informação, usuários e sistemas de informação deverão ser segregados em redes, sempre que possível.

Art. 76 A rede de convidados deverá possuir um sistema de autenticação garantindo que apenas usuários autorizados realizem o acesso, colaborando também com a rastreabilidade de eventos da rede.

Art. 77 As políticas e os procedimentos para transferência de informação dentro ou entre unidades do IF Sudeste MG, e com entidades externas, deverão ser estabelecidos visando proteger a informação, por meio do uso de todos os tipos de recursos de comunicação.

Art. 78 Os acordos de confidencialidade e não divulgação de informações deverão ser identificados, analisados criticamente e documentados garantindo os requisitos de proteção da informação.

Art. 79 O compartilhamento de dados com outros órgãos ou entidades da Administração Pública deve ser pautado na legislação vigente, considerando as restrições de acesso e sigilo, cabendo ao IF Sudeste MG definir os níveis adequados de segurança, por meio de normas complementares.

Seção VIII
Controles de Acesso

Art. 80 O acesso às redes e serviços computacionais pelos usuários serão autorizados mediante critérios estabelecidos em norma complementar.

Art. 81 Deverá ser implementado processo formal de registro e cancelamento de usuário para permitir atribuição dos direitos de acesso.

Art. 82 Contas inativas deverão ser consideradas nos processos de revogação de acesso, estabelecendo um período de inatividade máximo para que sejam desabilitadas.

Art. 83 Um processo formal de provisionamento de acesso do usuário também deverá ser implementado para conceder ou revogar os direitos de acesso em todos os tipos de sistemas e serviços.

Art. 84 O acesso privilegiado aos sistemas e serviços será restrito e controlado por meio de um processo de autorização formal.

Art. 85 Os gestores de ativos de informação deverão analisar periodicamente os direitos de acesso dos usuários.

Parágrafo único: É de responsabilidade da Diretoria de Gestão de Pessoas comunicar aos gestores de ativos de informação a exoneração de servidores, bem como o término dos contratos dos docentes substitutos.

Art. 86 O acesso à informação e às funções dos sistemas será restrito, de acordo com as normas de controle de acesso.

Art. 87 O gerenciamento de senhas será interativo e deverá assegurar senhas de qualidade, contendo os seguintes padrões de robustez quando suportado:

I – mínimo de 08 (oito) caracteres;
II – letras maiúsculas, minúsculas, números e caracteres especiais;
III – frases e/ou palavras impessoais; e
IV – combinações de caracteres variados, evitando padrões previsíveis, como dados pessoais, repetição de caracteres ou sequências numéricas.

Art. 88 As senhas definidas devem ser diferentes das últimas 05 (cinco) anteriores, impedindo que o usuário reutilize suas senhas recentes, quando suportado.

Art. 89 As senhas definidas devem ser alteradas após o período de 90 (noventa) dias, quando suportado.

Art. 90 Quando suportado, os acessos à aplicações expostas externamente, o acesso à rede e o acesso administrativo devem ser protegidos por autenticação multifator (MFA).

Art. 91 O usuário é responsável pelas atividades geradas pelas suas credenciais, respondendo por qualquer ação indevida realizada através de seu acesso.

Art. 92 As credenciais de acesso fornecidas são individuais e intransferíveis.

Art. 93 Os programas utilitários que necessitem sobrepor controles de segurança dos sistemas e aplicações serão restritos e estritamente controlados.

Art. 94 O acesso ao código-fonte de sistemas e aplicações será restrito às Equipes de Desenvolvimento, a ETIR em caso de incidentes cibernéticos e demais membros da equipe de TIC mediante aprovação formal.

Seção IX
Gestão de Riscos

Art. 95 Deverá ser estabelecido o processo de Gestão de Riscos de Segurança da Informação (GRSI) com vistas a minimizar possíveis impactos associados aos ativos de informação, possibilitando a seleção e a priorização dos ativos de informação a serem protegidos, bem como a definição e a implementação de controles para a identificação e o tratamento de possíveis falhas de segurança.

Art. 96 O IF Sudeste MG, conforme a GRSI, irá dimensionar e aplicar os investimentos necessários em medidas de segurança, segundo o valor do ativo de informação que está sendo protegido e de acordo com a identificação de riscos de potenciais prejuízos ao negócio, à atividade fim e aos objetivos institucionais**.**

Seção X
Gestão de Continuidade do Negócio

Art. 97 Deverá ser estabelecida a Gestão de Continuidade de Negócio no âmbito do IF Sudeste MG visando reduzir a possibilidade de interrupção causada por desastres ou falhas graves nos recursos que suportam as operações críticas do Instituto.

Seção XI
Auditoria e Conformidade

Art. 98 O cumprimento desta POSIN deve ser avaliado, periodicamente, pela alta direção, em conformidade com Normas Complementares, Manuais de Procedimentos e legislação específica de SI, buscando a certificação do atendimento dos requisitos de segurança da informação. A alta direção poderá se valer de grupos internos ou externos para consecução de auditorias.

Seção XII
Educação e Conscientização

Art. 99 Esta Política, as normas e procedimentos complementares devem ser periodicamente divulgados a todos os agentes públicos do IF Sudeste MG.

Art. 100 O IF Sudeste MG deverá manter programa contínuo de conscientização dos agentes públicos no tema segurança da informação, promovendo conhecimentos sobre engenharia social, práticas de autenticação, práticas de tratamento de dados e outros aspectos relevantes. Os conteúdos dispostos neste programa devem ser revisados periodicamente, adequando às necessidades atuais.

Art. 101 O Instituto deverá manter plano de capacitação aos servidores que atuam na gestão e nos temas relacionados à Segurança da Informação.

CAPÍTULO VII
DAS DISPOSIÇÕES FINAIS

Art. 102 A implementação das diretrizes dispostas na POSIN dependerá da disponibilidade de recursos financeiros, humanos e tecnológicos do IF Sudeste MG.

Art. 103 As questões relacionadas à gestão de vulnerabilidades tratadas no Art. 71 darão prioridade, inicialmente, aos ativos críticos do IF Sudeste MG.

Art. 104 A POSIN deverá ser revisada e atualizada periodicamente no máximo a cada 2 (dois) anos, caso não ocorram eventos ou fatos relevantes que exijam uma revisão imediata.

Art. 105 A presente Política deve ser lida em conjunto com as obrigações previstas nas normativas internas e documentos correlatos ao tema.

Art. 106 O descumprimento das disposições constantes nesta política, nas normas e nos procedimentos sobre segurança da informação caracteriza infração funcional, a ser apurada em processo administrativo disciplinar, sem prejuízo das responsabilidades penal e civil.

Art. 107 Casos omissos, os quais não estão cobertos por esta política, deverão ser submetidos ao Comitê de Segurança da Informação e Comunicação em exercício para que haja apreciação, definindo assim se o objeto será incluído ou resultará na alteração de algum ponto da política em vigência pelo Conselho de Governança Digital (COGD).