

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO
POSIC

MINAS GERAIS, 2023

HISTÓRICO DE VERSÕES

Data	Versão	Descrição	Autor
08/05/2023	1.01	Minuta Política de Segurança da Informação e Comunicação	Consultoria

SUMÁRIO

ESCOPO	3
OBJETIVOS	3
PRINCÍPIOS	4
DIRETRIZES GERAIS	4
DAS COMPETÊNCIAS E RESPONSABILIDADES	9
DAS PENALIDADES	12
DA ATUALIZAÇÃO	12
DAS DISPOSIÇÕES FINAIS	12
ANEXO I	13
ANEXO II	14

ESCOPO

Art. 1º Instituir a Política de Segurança da Informação e Comunicação, no âmbito do Instituto Federal de Educação, Ciência e Tecnologia do Sul de Minas Gerais - IFSULDEMINAS ("Instituição", "IFSULDEMINAS"), e suas unidades a saber: Reitoria, Campus Inconfidentes, Machado, Muzambinho, Passos, Poços de Caldas, Pouso Alegre, Três Corações e Carmo de Minas, com a finalidade de estabelecer princípios e diretrizes para a implementação de ações de segurança da informação e, no que couber, no relacionamento com outros órgãos públicos ou entidades privadas.

§ 1º Todos os instrumentos normativos gerados a partir da Política de Segurança da Informação e Comunicação do IFSULDEMINAS e suas unidades são partes integrantes desta Política e emanam dos princípios e diretrizes nela estabelecidos.

§ 2º As diretrizes de segurança da informação previstas nesta Política e nas demais normas específicas de segurança da informação da Instituição são aplicadas à toda comunidade interna e externa, conforme definição dada no Anexo I (conceitos e definições), que tenham acesso às informações e aos recursos de Tecnologia da Informação desta Instituto.

OBJETIVOS

Art. 2º A Política de Segurança da Informação e Comunicação do IFSULDEMINAS tem como objetivos:

- I - nortear a elaboração das normas necessárias à efetiva implementação da segurança da informação;
- II - estabelecer princípios e diretrizes a fim de proteger ativos de informação e conhecimentos gerados ou recebidos;
- III - estabelecer orientações gerais de segurança da informação e, desta forma, contribuir para a gestão eficiente dos riscos, limitando-os a níveis aceitáveis, bem como preservar os princípios da disponibilidade, integridade, confiabilidade e autenticidade das informações; e
- IV - estabelecer competências e responsabilidades quanto à segurança da informação.

PRINCÍPIOS

Art. 3º As ações de segurança da informação do IFSULDEMINAS são norteadas pelos princípios constitucionais e administrativos que norteiam a Administração Pública Federal, bem como pelos seguintes princípios:

I - disponibilidade, integridade, confidencialidade e autenticidade das informações, não repúdio;

II - continuidade dos processos e serviços essenciais para o funcionamento do Instituto;

III - responsabilidade das comunidades interna e externa, constituída no dever de conhecer e respeitar a Política de Segurança da Informação e Comunicação do Instituto e demais normas específicas de segurança da informação;

IV - alinhamento estratégico da Política de Segurança da Informação e Comunicação do Instituto com o planejamento estratégico do Instituto, assim como demais normas específicas de segurança da informação da Administração Pública Federal;

V - conformidade das normas e das ações de segurança da informação com a legislação e regulamentos aplicáveis; e

VI - educação e comunicação como alicerces fundamentais para o fomento da cultura em segurança da informação.

DIRETRIZES GERAIS

Art. 4º Estas diretrizes constituem os principais pilares da gestão de segurança da informação no IFSULDEMINAS, norteando a elaboração de políticas, planos e normas complementares no âmbito do Instituto e objetivam a garantia dos princípios básicos de segurança da informação estabelecidos nesta Política.

Art. 5º As normas, procedimentos, manuais e metodologias de segurança da informação do Instituto devem considerar, como referência, além das citadas no Anexo II, a legislação vigente, as melhores práticas de segurança da informação e os guias e orientações do governo federal acerca da temática.

Art. 6º As ações de segurança da informação devem:

I - considerar prioritariamente, os objetivos estratégicos, os planos institucionais, a estrutura e a finalidade do IFSULDEMINAS;

II - ser tratadas de forma integrada, respeitando as especificidades e autonomia dos campi;

III - ser adotadas proporcionalmente aos riscos existentes e à magnitude dos danos potenciais, considerados o ambiente, o valor e a criticidade da informação; e

IV - visar à prevenção da ocorrência de incidentes.

Art. 7º O investimento necessário em medidas de segurança da informação deve ser dimensionado segundo o valor do ativo a ser protegido e de acordo com o risco de potenciais prejuízos para o Instituto.

Parágrafo único. O planejamento de investimentos para a segurança da informação deve constar no Plano Diretor de Tecnologia da Informação do Instituto.

Art. 8º Toda e qualquer informação gerada, custodiada, tratada, utilizada ou armazenada no Instituto e suas unidades compõem o seu ativo da informação e deve ser protegida conforme normas em vigor estabelecidas no âmbito do Instituto, e, no que couber, conforme normativos constantes do Anexo II.

Art. 9º Pessoas e sistemas devem ter o menor privilégio e o mínimo acesso aos recursos necessários para realizar uma dada tarefa.

Parágrafo único. É condição para acesso aos recursos de tecnologia da informação do IFSULDEMINAS a assinatura de Termo de Responsabilidade ou similar, contendo minimamente ciência aos termos desta Política, as responsabilidades e compromissos em decorrência deste acesso e penalidades cabíveis pela inobservância das regras previstas nas normas de segurança da informação do Instituto .

Art. 10. Esta Política de Segurança da Informação e Comunicação e suas atualizações, bem como normas específicas de segurança da informação do IFSULDEMINAS, deverão ser divulgadas amplamente a toda comunidade interna e externa, ainda que a atuação no Instituto seja temporária, a fim de promover sua observância, seu conhecimento, bem como a formação da cultura de segurança da informação.

§ 1º Toda comunidade interna deve ser continuamente capacitada nos procedimentos de segurança, inclusive com campanhas, e no uso correto dos ativos de informação quando da realização de suas atribuições, de modo a minimizar possíveis riscos à segurança da informação.

Art. 11. Todos os contratos de prestação de serviços, convênios e acordos de cooperações, firmados pelo IFSULDEMINAS conterão cláusula específica sobre a obrigatoriedade de atendimento às diretrizes desta Política de Segurança da Informação e Comunicação.

Art. 12. A aplicação desta Política de Segurança e Comunicação requer que seus efeitos sejam evidenciados, monitorados e controlados por um instrumento de gestão adequado.

Art. 13. Um SGSI – Sistema de Gestão da Segurança da Informação – adequado como disposto nesta POSIC deverá ser mantido continuamente;

Art. 14. A estrutura do Sistema de Gestão de Segurança da Informação do IFSULDEMINAS é composta por:

I – o Gestor de Segurança da Informação;

II – a(s) equipe(s) de tratamento e resposta a incidentes em redes computacionais; e

III – os comitês e subcomitês de segurança da informação.

§ 1º A Política de Segurança da Informação e Comunicação integra o arcabouço legal do Sistema de Gestão de Segurança da Informação do Instituto.

§ 2º A estrutura do Sistema de Gestão de Segurança da Informação do Instituto deverá estar em conformidade com o Plano de Desenvolvimento Institucional.

Art. 15. Gestão de riscos de SI

§ 1º A Gestão de Riscos de Segurança da Informação deverá integrar-se às metodologias e normativos de gestão de risco institucional e suas unidades possibilitando a identificação, a quantificação, a priorização, o tratamento, a comunicação e a monitoração periódica dos riscos de SI, contemplando minimamente os seguintes documentos:

I – plano de gestão de riscos de segurança da informação;

II – relatório de identificação, análise e avaliação dos riscos de segurança da informação; e

III – relatório de tratamento de riscos de segurança da informação.

§ 1º As unidades do IFSULDEMINAS deverão implementar e executar as atividades de gestão de riscos de segurança da informação associados aos ativos de informação sob sua responsabilidade.

§ 2º Os riscos de SI deverão ser considerados durante o planejamento, na execução, monitoramento e na finalização da contratação de bens e serviços. Deverá atribuir-se às responsabilidades aos gestores, fiscais e fornecedores acerca da SI.

Art. 16. Gestão de ativos

§ 1º A Estrutura de SI do IFSULDEMINAS, deverá instituir políticas, normas e procedimentos que estabeleçam o controle de gestão de ativos em seus respectivos locais.

Art. 17. Gestão de continuidade de negócio

§ 1º A Estrutura de SI do Instituto e suas unidades, em conjunto com as áreas responsáveis pelos ativos de informação, deverão instituir normas, procedimentos e controles que

§ 2º Estabeleçam a gestão de continuidade do negócio, a fim de minimizar os impactos decorrentes de potenciais eventos que causem a indisponibilidade sobre os serviços de TI do IFSULDEMINAS.

§ 3º A Estrutura de SI do IFSULDEMINAS, deverá instituir políticas, normas e procedimentos que estabeleçam a gestão de continuidade.

ART. 18 Gestão de incidentes cibernéticos

§ 1º A Estrutura de SI do Instituto e suas unidades deverão criar e manter uma Equipe de Tratamento e Resposta a Incidentes Cibernéticos (ETIR), instituída pela alta gestão, com a responsabilidade de coordenar as atividades relacionadas a incidentes cibernéticos.

§ 2º Os eventos e incidentes cibernéticos devem ser tratados de acordo com as ações e procedimentos específicos detalhados na atuação da ETIR-IFSULDEMINAS, no qual se definirá as responsabilidades e procedimentos para assegurar respostas tempestivas, efetivas e ordenadas perante incidentes de SI de forma a contribuir para garantir a continuidade das

atividades com vistas a não intervenção no alcance dos objetivos estratégicos do Instituto e suas unidades.

§ 3º A constituição e regulamentação da ETIR será efetivada por meio de documento formal aprovado por instância competente do IFSULDEMINAS.

ART 19. Conformidade

§ 1º O cumprimento desta POSIC deverá ser avaliado periodicamente, por meio de verificações de conformidade realizadas com o apoio do Comitê de Segurança da Informação e Comunicações.

§ 2º Os normativos de SI devem ser analisados criticamente e verificados em períodos regulares, minimamente 2 (dois) anos ou sempre que necessário, pela Estrutura de SI do Instituto, tendo por base a conformidade com políticas, padrões, normas, ferramentas, manuais de procedimentos e outros documentos permanentes.

§ 3º A Estrutura de SI do Instituto e suas unidades devem instituir processos de análise e tratamento de conformidade, visando garantir o atendimento das leis, regulamentos e normas que regem as atividades no âmbito da Administração Pública Federal.

§ 4º O Processo de Avaliação da Conformidade será composto, no mínimo, pelos seguintes documentos:

- I - O plano de gestão de riscos de segurança da informação;
- II - O relatório de identificação, análise e avaliação dos riscos de segurança da informação; e
- III - O relatório de tratamento de riscos de segurança da informação.

ART 20. Segurança física e do ambiente

§ 1º O acesso físico aos ambientes de TI do IFSULDEMINAS deverá possuir controles e mecanismos de segurança adequados aos níveis de segurança exigidos para cada local.

§ 2º As instalações/infraestruturas – críticas ou sensíveis –, os processos e atividades que sustentam os serviços críticos de tecnologia da informação (TI) disponibilizados pelo Instituto e suas unidades devem ser protegidos, considerando os riscos identificados, os níveis de segurança definidos e os controles de segurança implementados de forma a garantir a

disponibilidade, integridade, autenticidade e confidencialidade das informações , bem como contra o acesso indevido, danos e interferências.

§ 3º A Estrutura de SI do IFSULDEMINAS, deverá instituir políticas, normas e procedimentos que estabeleçam o controle físico na Reitoria e nas demais unidades.

ART 21. Controles de acesso

§ 1º A Estrutura de SI do IFSULDEMINAS, deverá instituir políticas, normas e procedimentos que estabeleçam o controle de acesso aos ativos de informação em seus respectivos locais.

ART 22. Gestão do uso de recursos operacionais e de comunicações

§ 1º Os recursos computacionais e de comunicações do IFSULDEMINAS e suas unidades devem ser empregados para fins institucionais direta ou indiretamente relacionados a atividades institucionais e em obediência a esta política, aos princípios, diretrizes e legislações pertinentes que regem a administração pública federal.

§ 2º. Os usuários terão seus acessos autorizados conforme as políticas e normas de TI do IFSULDEMINAS.

DAS COMPETÊNCIAS E RESPONSABILIDADES

Art. 23. Cabe à alta administração do IFSULMINAS:

I – realizar a governança da segurança da informação, conforme competências estabelecidas em normativos vigentes do governo federal;

II – implantar os controles gerais de segurança da informação positivados nas normas do GSI/PR, Ministério da Gestão e da Inovação em Serviços Públicos, TCU e demais órgãos normatizadores ou de controles;

III – comprometer-se com o desenvolvimento e com a implementação do Sistema de Gestão de Segurança da Informação do Instituto, bem como com o tratamento das ações e decisões de segurança da informação em um nível de relevância e prioridade adequados;

IV – prover os recursos financeiros e materiais para a implementação e manutenção do Sistema de Gestão de Segurança da Informação do IFSULDEMINAS; e

V - designar ao menos um servidor efetivo, pertencente ao IFSULDEMINAS, como responsável pela avaliação de conformidade de acordo com os aspectos relativos à segurança da informação.

Art. 24. Cabe ao Comitê de Segurança da Informação e Comunicações do IFSULDEMINAS:

I - assessorar na implementação das ações de segurança da informação e comunicação;

II - constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação;

III - Participar da elaboração da política de segurança da informação e das normas internas de segurança da informação.

IV - Propor alterações à política de segurança da informação e às normas internas de segurança da informação.

V - Deliberar sobre normas internas de segurança da informação.

VI - Deliberar sobre as ações propostas pelo gestor de segurança da informação no parecer técnico sobre o relatório de avaliação de conformidade e encaminhar à alta administração para aprovação o processo contendo os documentos sobre a avaliação de conformidade.

Art. 25. Cabe ao Gestor de Segurança da Informação do IFSULDEMINAS:

I - Prestar contas das atividades de segurança da informação ao Comitê de Segurança da Informação ou estrutura equivalente;

II - Coordenar a elaboração da política de segurança da informação e das normas internas de segurança da informação, observadas as normas afins exaradas pelo GSI/PR e as melhores práticas sobre o assunto;

III - Assessorar a alta administração na implementação da política de segurança da informação;

IV - Estimular ações de capacitação e de profissionalização de recursos humanos em temas relacionados à segurança da informação;

V - Promover a divulgação da política e das normas internas de segurança da informação a todos os servidores, usuários e prestadores de serviços que trabalham no IFSULDEMINAS;

VI - Propor recursos necessários às ações de segurança da informação;

VII - Acompanhar os trabalhos da ETIR;

VIII - Verificar os resultados dos trabalhos de auditoria sobre a gestão da segurança da informação;

IX - Acompanhar a aplicação de ações corretivas e administrativas cabíveis nos casos de violação da segurança da informação;

X - Manter contato direto com o DSI/GSI/PR em assuntos relativos à segurança da informação;

XI - Coordenar os processos de realização obrigatória pelos órgãos normatizadores ou de controles;

XII - Coordenar a avaliação de conformidade nos aspectos relativos à segurança da informação; e

XIII - Emitir parecer técnico sobre o relatório de avaliação de conformidade e apresentá-los ao Comitê de Segurança da Informação.

Art. 26. Cabe ao agente responsável pela gestão dos ativos de informação do IFSULDEMINAS:

I - identificar e classificar os ativos de informação por nível de criticidade;

II - identificar potenciais ameaças aos ativos de informação;

III - identificar vulnerabilidades dos ativos de informação;

IV - consolidar informações resultantes da análise do nível de segurança da informação de cada ativo de informação ou de grupos de ativos de informação em um relatório;

V - autorizar a atualização do relatório mencionado no inciso IV do caput; e

VI - avaliar os riscos dos ativos de informação ou do grupo de ativos de informação.

Art. 27. Cabe ao(s) agente(s) responsável(is) pela avaliação de conformidade de Segurança da Informação do IFSULDEMINAS:

I - elaborar o plano de verificação de conformidade;

II - elaborar o relatório de avaliação de conformidade e remetê-lo ao gestor de segurança da informação; e

III - verificar a adequação dos procedimentos de segurança da informação de acordo com as recomendações descritas no relatório de avaliação de conformidade.

Art. 28. É responsabilidade de todos os gestores do Instituto o conhecimento, execução e a disseminação dessa Política e demais normas específicas de segurança da informação aos colaboradores que estão sob a sua gestão.

Art. 29. Toda a comunidade interna e externa é responsável pela segurança dos ativos de informação que estejam sob a sua responsabilidade.

DAS PENALIDADES

Art. 30. Ações que violem a Política de Segurança da Informação e Comunicação do IFSULDEMINAS poderão acarretar, isolada ou cumulativamente, nos termos da legislação aplicável, sanções administrativas, civis e penais, assegurados aos envolvidos o contraditório e a ampla defesa.

DA ATUALIZAÇÃO

Art. 31. A Política de Segurança da Informação e Comunicação do IFSULDEMINAS deverá ser revisada em função de alterações na legislação pertinente, de diretrizes políticas do Governo Federal, de alterações nos normativos do Instituto, quando considerada necessária pelo Comitê de Segurança da Informação e Comunicações do IFSULDEMINAS, ou a cada 2 (dois) anos a contar da data de sua publicação.

DAS DISPOSIÇÕES FINAIS

Art. 32. Questões relacionadas à Política de Segurança da Informação e Comunicação do Instituto e seus documentos devem ser submetidas ao Comitê de Segurança da Informação e Comunicações.

ANEXO I

CONCEITOS E DEFINIÇÕES

1. Para os fins da Política de Segurança da Informação e Comunicação do IFSULDEMINAS, fica estabelecido o significado dos seguintes termos e expressões baseados no “Glossário de Segurança da Informação” do governo federal, com os seguintes destaques complementos:

1.1. ativo de informação: meios de armazenamento, transmissão e processamento da informação, equipamentos necessários a isso, sistemas utilizados para tal, locais onde se encontram esses meios, recursos humanos que a eles têm acesso e conhecimento ou dado que tem valor para um indivíduo ou organização;

1.2. comunidade interna: todas as pessoas envolvidas com o desenvolvimento de atividades no IFSULDEMINAS de caráter permanente, continuado ou eventual, incluindo, prestadores de serviço, estagiários, servidores de carreira ou temporários, comissionados e aposentados;

1.3. comunidade externa: todas as pessoas assistidas pelos serviços prestados pelo IFSULDEMINAS, incluindo outros órgãos, empresas privadas e **alunos**;

1.4. diretrizes de segurança da informação: ações que definem a Política de Segurança da Informação e Comunicação do Instituto Federal do Sul de Minas, visando a preservar a disponibilidade, integridade, confiabilidade e autenticidade das informações da Instituição;

1.5. responsável pelo ativo de informação: servidor público responsável pela salvaguarda do ativo de informação;

1.6. risco: no sentido amplo, trata-se da possibilidade de ocorrência de um evento que pode impactar o cumprimento dos objetivos. Pode ser mensurado em termos de impacto e de probabilidade;

1.7. risco de segurança da informação: potencial associado à exploração de uma ou mais vulnerabilidades de um ativo de informação ou de um conjunto de tais ativos, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização; e

1.8. segurança da informação: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações.

ANEXO II

REFERÊNCIAS LEGAIS E NORMATIVAS

1. Esta norma foi elaborada em conformidade às seguintes referências legais e normativas:

1.1. Lei nº 12.527, de 18 de novembro de 2011, que regula o acesso a informações;

1.2. Decreto nº 10.849, de 28 de outubro de 2021, que altera o Decreto nº 9.637, de 26 de dezembro de 2018, para dispor sobre a composição do Comitê Gestor da Segurança da Informação.

1.3. Decreto nº 10.748, de 16 de julho de 2021, que institui a Rede Federal de Gestão de Incidentes Cibernéticos.

1.4. Decreto nº 10.641, de 2 de março de 2021, que altera o Decreto nº 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o Decreto nº 2.295, de 4 de agosto de 1997, que regulamenta o disposto no art. 24, caput, inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional.

1.5. Decreto Nº 10.332, de 28 de ABRIL de 2020, que institui a Estratégia de Governo Digital para o período de 2020 a 2022, no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional e dá outras providências.

1.6 - Portaria SGD/MGI Nº 852, de 28 de março de 2023 - Dispõe sobre o Programa de Privacidade e Segurança da Informação - PPSI.

1.7. Portaria Nº 93 GSI/PR, de 18 de outubro de 2021, que aprova o Glossário de Segurança da Informação.

1.8. Instrução Normativa SGD/ME Nº 94, de 23 de dezembro de 2022, que dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação - TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal.

- 1.9. Instrução Normativa Conjunta MP/CGU n. 01, de 2016, que dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo Federal.
- 1.10. Instrução Normativa GSI Nº 1 - 27 de maio de 2020 - Dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal.
- 1.11. Instrução Normativa GSI Nº 3 - 28 de maio de 2021 - Dispõe sobre os processos relacionados à gestão de segurança da informação na APF.
- 1.12. Instrução Normativa GSI Nº 6 - 23 de dezembro de 2021 - Estabelece diretrizes de segurança da informação para o uso seguro de mídias sociais nos órgãos e nas entidades da administração pública federal.
- 1.13. NC nº 05 /IN01/DSIC/GSIPR - Disciplina a criação de Equipes de Tratamento e Respostas a Incidentes em Redes Computacionais - ETIR na APF.
- 1.14. NC nº 08 /IN01/DSIC/GSIPR - Estabelece as Diretrizes para Gerenciamento de Incidentes em Redes Computacionais na APF.
- 1.15. NC nº 12 /IN01/DSIC/GSIPR - Estabelece diretrizes e orientações básicas para o uso de dispositivos móveis nos aspectos referentes à Segurança da Informação e Comunicações (SIC) nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta.
- 1.16. NC nº 17 /IN01/DSIC/GSIPR - Estabelece Diretrizes nos contextos de atuação e adequações para Profissionais da Área de Segurança da Informação e Comunicações (SIC) nos Órgãos e Entidades da Administração Pública Federal (APF).
- 1.17. NC nº 20 /IN01/DSIC/GSIPR - Estabelece as Diretrizes de Segurança da Informação e Comunicações para Instituição do Processo de Tratamento da Informação nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta.
- 1.18. NC nº 21 /IN01/DSIC/GSIPR - Estabelece as Diretrizes para o Registro de Eventos, Coleta e Preservação de Evidências de Incidentes de Segurança em Redes na APF.
- 1.19. Acórdão TCU 1768/2022 - Plenário, versa acerca de segurança cibernética de instituições federais.

1.20. Brasil. Tribunal de Contas da União. Cinco controles de segurança cibernética para ontem
Tribunal de Contas da União. – Brasília : TCU, 2022.

1.21. Brasil. Cartilha de Gestão de Segurança da Informação. – Brasília : DSI/GSI/PR, 2022.