SERVIÇO PÚBLICO FEDERAL

MINISTÉRIO DA EDUCAÇÃO

SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA SUL-RIO-GRANDENSE

RESOLUÇÃO CONSUP/IFSUL Nº 137, de 18 de maio de 2022.

Aprova a Política de Segurança da Informação do IFSul - POSIN.

O Presidente do Conselho Superior do Instituto Federal de Educação, Ciência e Tecnologia Sul-rio-grandense, no uso das atribuições legais que lhe confere a Lei Nº 11.892, de 29 de dezembro de 2008, e conforme deliberação do Conselho Superior na reunião ordinária realizada no dia 17 de maio de 2022, resolve:

Art. 1º Aprovar a Política de Segurança da Informação do IFSul - POSIN.

Art. 2º Esta Resolução entra em vigor na data de sua publicação.

Flavio Luis Barbosa Nunes

Presidente do CONSUP

Documentos Anexados:

- **Anexo #1.** Política de Segurança da Informação do IFSul (anexado em 18/05/2022 15:53:55)

Política de Segurança da Informação do IFSul - POSIN

DESENVOLVIDO POR:
COMITÊ GOVERNANÇA DIGITAL - CGD

2022

CONTROLE DO DOCUMENTO

Armazenamento do Documento

Título do Documento	Política de Segurança da Informação e Comunicações
Localização do Documento	Portal institucional - ifsul.edu.br
Formato do Documento	PDF

Elaboração da Minuta

Nome	**Cargo**	**Data**	**Versão**
Carla Simone Guedes Pires	Diretora de TI	28/02/2022	V 0,1

Aprovações

	Data	Versão
CGD	20/04	0,1
Revisão	02/05	1,0
CONSUP		1.1
Publicação		1.1

Política de Segurança da Informação do IFSul - POSIN

CAPITULO I

DISPOSIÇÕES GERAIS

Art. 1º. A Política de Segurança da Informação (POSIN) do IFSul está baseada nas recomendações da norma ABNT NBR ISO/IEC 27002:2005, reconhecida mundialmente como um código de prática para a gestão da segurança da informação, além de estar de acordo com o Decreto nº9.637de 26/12/2018, que institui a Política Nacional de Segurança da Informação nos órgãos e entidades da Administração Pública Federal, e outras leis vigentes.

Parágrafo Único. A POSIN apresenta o compromisso institucional com a proteção das informações de sua propriedade e/ou sob sua guarda, devendo ser cumprida por todos os servidores, colaboradores, consultores externos, estagiários, bolsistas, prestadores de serviço ou quem possua acesso a dados e informações no âmbito do IFSul.

Art. 2º A POSIN tem por objetivo estabelecer diretrizes e responsabilidades adequadas para o manuseio, tratamento, controle e proteção dos ativos de informação pertinentes ao IFSul, em conformidade com a legislação vigente, com os valores éticos e com as melhores práticas de segurança da informação. Desse modo, a POSIN busca preservar os ativos de informação pertencentes ao IFSul, assim como a sua imagem institucional.

CAPÍTULO II

DO ESCOPO E ABRANGÊNCIA

Art. 3º A Política de Segurança da Informação é composta por diretrizes, normas, procedimentos e responsabilidades adequadas para manuseio, tratamento, controle e proteção das informações pertinentes ao IFSul.

Art. 4º As diretrizes, as normas complementares, os manuais e os procedimentos de segurança da informação contidos nesta Política de Segurança da Informação aplicam-se a todos os usuários dos ativos de informação do IFSul, independentemente do tipo de vínculo, nível hierárquico ou função.

CAPÍTULO III

DA CONCEITUAÇÃO

Art. 5º Para fins de uniformidade dos procedimentos contidos nesta POSIN, são adotados os conceitos a seguir:

I - Ativo: tudo que manipula a informação, inclusive ela própria, tais como processos administrativos, bases de dados e arquivos, documentação de sistema, manuais, material de treinamento, procedimentos de suporte ou operação, planos de continuidade, procedimentos de recuperação, informações armazenadas, softwares, sistemas, ferramentas de desenvolvimento e utilitários, estações de trabalho, servidores, equipamentos de comunicação, no-breaks e outros. Qualquer bem, tangível ou intangível, que tenha valor para o IFSul.

II - Ativo de informação: ativo que guarda informações do IFSul.

III - Autenticidade: garantia de que o acesso e o tráfego de dados ocorrem através de canais seguros e provêm de fontes verdadeiras, conforme anunciadas, tanto na origem como no destino.

IV – Integridade: Consiste na fidedignidade de informações. Sinaliza a conformidade de dados armazenados com relação às inserções, alterações e processamentos autorizados efetuados.

V - Confidencialidade: garantia do acesso reservado ao ativo de informação, de acordo com seu nível de proteção, cuja classificação será regulada em norma específica.

VI - Disponibilidade: garantia de que os usuários possam ter acesso a informações segundo sua demanda. Pode ser crítica, que exige recuperação imediata em caso de perda, ou normal, quando a recuperação pode se dar em espaço de tempo maior.

VII - Incidente de Segurança da Informação: qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de informação, levando à perda de um ou mais princípios básicos de Segurança da Informação: autenticidade, confidencialidade, integridade e disponibilidade.

VIII - Informação: resultante de processamento, manipulação e organização de dados, de tal forma que represente uma modificação (quantitativa ou qualitativa) no conhecimento do sistema (humano, animal ou máquina) que a recebe.

IX- Integridade: garantia de que as informações mantêm as características originais definidas pelo proprietário. Os métodos de processamento e as atividades de alteração da informação devem ser planejados e autorizados, ocorrendo de forma básica, sem registro de log, ou com trilha de auditoria.

X - Medidas de proteção: medidas destinadas a garantir o sigilo, quando necessário, a inviolabilidade, a integridade, a autenticidade, a legitimidade e a disponibilidade de

dados e informações, com o objetivo de prevenir, detectar, anular ou registrar ameaças reais ou potenciais a dados e informações.

XI - Não-repúdio: garantia de que o emissor da mensagem não irá negar posteriormente a autoria da mensagem ou transação, permitindo a sua identificação.

XII- Política de Segurança da Informação: conjunto de princípios que norteiam a gestão de segurança de informações e que deve ser observado pelo corpo técnico e gerencial e pelos usuários internos e externos da instituição. As diretrizes estabelecidas nesta política determinam as linhas mestras que devem ser seguidas pela instituição para que sejam assegurados seus recursos computacionais e suas informações.

XIII- Prestadores de Serviço: pessoa jurídica ou física que mantenha contrato de prestação de serviço no IFSul.

XIV - Proprietário da Informação: responsável pela classificação e autorização do acesso à informação.

XV - Segurança da Informação: conjunto de controles que visam garantir a preservação dos aspectos de confidencialidade, integridade e disponibilidade das informações.

XVI - Sigilo: propriedade da informação que indica o impedimento de acesso a ela por pessoa não autorizada.

XVII - Termo de Responsabilidade: documento que formaliza a obrigação de servidores e colaboradores quanto a guarda e tratamento das informações, de acordo com seu nível de confidencialidade estabelecido pelo proprietário, e a correta utilização dos recursos computacionais disponibilizados pelo IFSul, de acordo com o estabelecido em normas específicas.

XVIII - Usuário: são as pessoas que utilizam os recursos e serviços de tecnologia da informação (TI) no dia a dia, podendo ser titular de cargo efetivo, contratado por tempo determinado, prestador de serviço terceirizado, estagiários, alunos e voluntários.

CAPÍTULO IV

DOS PRINCÍPIOS

Art. 6º O IFSul atua em conformidade com os procedimentos estabelecidos nesta POSIN, observando os princípios da legalidade, da impessoalidade, da moralidade, da publicidade, da eficiência, da finalidade, do interesse público, da transparência e da motivação dos atos administrativos, exonerando-se de toda e qualquer responsabilidade decorrente do uso indevido, negligente ou imprudente dos recursos e serviços concedidos aos seus usuários, reservando-se o direito de analisar dados e evidências para obtenção de provas a serem utilizadas em processos investigatórios, bem como adotar as medidas legais cabíveis.

§ 1º Todas as informações produzidas ou recebidas pelos servidores, colaboradores, fornecedores e prestadores de serviço, em resultado do exercício de sua função e/ou atividade profissional contratada, pertence ao IFSul, as exceções devem ser formalizadas explicitamente entre as partes.

§ 2º Todos os ativos de informação do IFSul, inclusive os recursos computacionais, devem ser utilizados de forma responsável, consciente e aplicados na consecução dos objetivos institucionais do IFSul.

§ 3º Os sistemas, recursos e aplicações informacionais do IFSul serão utilizados mediante controle de acessos gerenciados e monitorados com apoio de ferramentas tecnológicas adequadas e mediante processos suficientemente definidos com vistas a assegurar a devida proteção dos ativos de informação e da infraestrutura computacional da instituição. Pessoas e sistemas devem ter o menor privilégio e o mínimo acesso aos recursos necessários para realizar uma dada tarefa.

§ 4º Cada usuário é individualmente responsável pela segurança das informações dentro da organização, principalmente daquelas que estejam sob sua guarda ou responsabilidade.

§ 5º Com o objetivo de reduzir o risco de descontinuidade das atividades da instituição e de perda de confidencialidade, integridade e disponibilidade dos ativos de informação, serão implantados e gerenciados planos de contingência e de continuidade para os principais serviços e sistemas – tais planos serão implantados, revisados e testados periodicamente.

§ 6º Quando o objeto for pertinente, deverá constar em todos os contratos celebrados pela instituição, cláusula de confidencialidade e de obediência às normas internas de Segurança da Informação a ser observada pelas empresas fornecedoras e por todos os profissionais que vierem a desempenhar atividades profissionais no âmbito dos respectivos contratos, inclusive aqueles firmados junto a organismos internacionais.

CAPÍTULO V

DOS REQUISITOS LEGAIS

Art. 7º As Diretrizes Básicas da Política de Segurança da Informação devem atender às seguintes normas:

I - Lei nº 12.527, de 18 de novembro de 2011, que dispõe sobre o acesso à informação pública.

II - Decreto no 7.724, de 16 de maio de 2012, que regulamenta o acesso à informação pública.

III - 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

IV - Lei nº 9.983, de 14 de julho de 2000, que dispõe sobre a responsabilidade civil e criminal de usuários que cometam irregularidades em razão do acesso a dados, informações e sistemas informatizados da Administração Pública.

V - Decreto nº 3.505, de 13 de junho de 2000, que institui a Política de Segurança da Informação nos órgãos e entidades de Administração Pública Federal.

VI - Artigo 307 do Código Penal Brasileiro (Decreto-Lei no 2.848, de 7 de dezembro de 1940), que pune a falsa identidade.

VII - Norma ABNT NBR ISO/IEC 27001:2006, que provê um modelo para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um Sistema de Gestão de Segurança da Informação (SGSI).

VIII- Norma ABNT NBR ISO/IEC 27037:2013, que fornece diretrizes para atividades específicas no manuseio de evidências digitais que são a identificação, coleta, aquisição e preservação de evidência digital que possam possuir valor probatório.

IX - Norma ABNT NBR ISO/IEC 27002:2013, que fornece diretrizes para práticas de gestão de segurança da informação e normas de segurança da informação para as organizações, incluindo a seleção, a implementação e o gerenciamento de controles, levando em consideração os ambientes de risco da segurança da informação da organização.

X - Norma ABNT NBR ISO/IEC 27003:2020, que fornece explicações e orientações sobre a ABNT NBR ISO/IEC 27001:2013.

XI - Norma ABNT NBR ISO/IEC 27007:2018, que fornece diretrizes sobre como gerenciar um programa de auditoria de Sistemas de Gestão da Segurança da Informação (SGSI), sobre como executar as auditorias e sobre a competência dos auditores de SGSI.

XII - Norma ABNT NBR ISO/IEC 27014:2013, que fornece orientação sobre conceitos e princípios para a governança de segurança da informação, pela qual as organizações podem avaliar, dirigir, monitorar e comunicar as atividades relacionadas com a segurança da informação dentro da organização.

XIII - Norma ABNT NBR ISO/IEC 27032:2015, que fornece diretrizes para melhorar o estado de Segurança Cibernética, traçando os aspectos picos desta atividade e suas ramificações em outros domínios de segurança.

XIV- Norma ABNT NBR ISO/IEC 27018:2018, que estabelece objetivos de controle, controles e diretrizes comumente aceitos para implementação de medidas para proteger as Informações de Identificação Pessoal (PII) de acordo com os princípios de privacidade descritos na ISO/IEC 29100, para o ambiente de computação em nuvem pública.

XV - Norma ABNT NBR ISO/IEC 16167:2013, que estabelece as diretrizes básicas para classificação, rotulação e tratamento das informações de acordo com sua sensibilidade e criticidade para a organização, visando ao estabelecimento de níveis adequados de proteção.

XVI - Norma ABNT NBR ISO/IEC 22301:2013, que especifica os requisitos para planejar, estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar continuamente um sistema de gestão documentado para se proteger, reduzir a possibilidade de ocorrência, preparar-se, responder e recuperar-se de incidentes de interrupção quando estes ocorrerem.

XVII - Norma ABNT NBR ISO/IEC 29100:2020, que fornece uma estrutura de privacidade que especifica uma terminologia comum de privacidade; específica os atores e os seus papéis no tratamento de dados pessoais (DP); descreve considerações de salvaguarda de privacidade; e fornece referências para princípios conhecidos de privacidade para tecnologia da informação.

CAPÍTULO VI

DAS DIRETRIZES BÁSICAS

Art. 8º As Diretrizes Básicas da Política de Segurança da Informação devem ser divulgadas nos setores institucionais, garantindo que todos tenham consciência da política e as pratiquem dentro do IFSul. São elas:

I- O IFSul deve instituir formalmente um responsável pela segurança da informação na organização, conforme orientação contida na NBR ISO/IEC 27.002.

II - A Gestão de Segurança da Informação do IFSul deve auxiliar a alta administração na priorização de ações e investimentos com vistas à correta aplicação de mecanismos de proteção, tendo como base as orientações estratégicas e as necessidades operacionais prioritárias da instituição e as implicações que o nível de segurança poderá trazer ao cumprimento dessas exigências.

III - O IFSul deve se orientar pelas melhores práticas e procedimentos de segurança da informação, recomendados por órgãos e entidades públicas e privadas responsáveis pelo estabelecimento de padrões de segurança da informação.

IV - O IFSul deve assegurar que os usuários entendam suas responsabilidades e estejam de acordo com os seus papéis para prevenir fraudes, roubos ou mau uso dos recursos públicos.

V - As medidas de proteção devem ser planejadas e os custos na aplicação de controles devem ser balanceados de acordo com os danos potenciais de falhas de segurança.

VI - O IFSul deve criar, gerir e avaliar critérios de tratamento e classificação da informação de acordo com o sigilo requerido, relevância, criticidade e sensibilidade, observando a legislação em vigor.

VII - Os incidentes de segurança da informação devem ser identificados, monitorados, comunicados e devidamente tratados de forma a impedir a interrupção das atividades e não afetar o alcance dos objetivos estratégicos.

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

IX - Deve ser estabelecida a Gestão de Continuidade de Negócio no âmbito do IFSul visando reduzir a possibilidade de interrupção causada por desastres ou falhas graves nos recursos que suportam as operações críticas da instituição.

X - O cumprimento desta POSIN deve ser avaliado, periodicamente, pela alta direção, em conformidade com normas complementares, manuais de procedimentos e legislação específica de Sistemas de Informação (SI), buscando a certificação do atendimento dos requisitos de segurança da informação.

Comentado [UC1]: Escrevi Sistemas de Informação

XI- Devem ser instituídas normas complementares à POSIN que estabeleçam procedimentos, processos e mecanismos que garantam o controle de acesso às informações, instalações e sistemas de informação.

XII - Ações de segurança deverão garantir a operação segura e correta dos recursos de processamento da informação do IFSul. As informações e os recursos de processamento de informação deverão ter controles específicos que garantam sua integridade e sua disponibilidade. As trocas de informações, tanto internamente quanto externamente, deverão ser reguladas de forma a manter o nível adequado da segurança da informação. As operações deverão ser adequadamente monitoradas de forma a detectar atividades não autorizadas.

XIII - Os ativos da organização devem ser protegidos contra acesso físico não autorizado, danos, perdas, furto e interferência. As proteções devem estar alinhadas aos riscos identificados.

CAPÍTULO VII

DO TRATAMENTO DE DADOS PESSOAIS

Art. 9º O tratamento de dados pessoais obedecerá ao regramento da LEI Nº 13.709, DE 14 DE AGOSTO DE 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) somente poderá ser realizado nas seguintes hipóteses:

Parágrafo único. Tratamento de dados é toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

I. Para atender aos interesses legítimos da instituição, cumprimento de obrigação legal ou regulatória.

II. Mediante o fornecimento de consentimento pelo titular.

III. Para execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições.

IV. Para realização de estudos referente a pesquisas, garantida, sempre que possível, a anonimização dos dados pessoais.

V. O tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização.

Art. 10º No legítimo interesse institucional fundamentado nas finalidades legítimas, baseado somente nos dados pessoais estritamente necessários para a finalidade pretendida.

Art. 11º O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso:

I. Finalidade específica do tratamento.

II. Forma e duração do tratamento.

III. Identificação do controlador.

IV. Informações de contato do controlador.

V. Informações acerca do uso compartilhado de dados pelo controlador e a finalidade.

VI. Responsabilidades dos agentes que realizarão o tratamento.

VII. Direitos do titular, com menção explícita aos direitos.

CAPÍTULO VIII
DO TRATAMENTO DE DADOS PESSOAIS SENSÍVEIS

Art. 12º O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:

§ 1º. Para finalidades específicas, execução de políticas públicas e cumprimento de obrigação legal ou regulatória previstas em leis:

I Realização de estudos em pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis.

II Exercício regular de direitos, inclusive em contrato e em processo administrativo.

§ 2º. Os dados anonimizados não serão considerados dados pessoais para os fins da LGPD, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido.

§ 3º Poderão ser igualmente considerados como dados pessoais sensíveis, aqueles utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada.

§ 4º A divulgação de resultados ou de qualquer excerto do estudo ou da pesquisa em nenhuma hipótese poderá revelar dados pessoais.

§ 5º O responsável por coletas de dados em pesquisa será o responsável pela segurança da informação destes, não será permitida, em circunstância alguma, a transferência dos dados a terceiro.

§ 3º. Para fins de esclarecimentos, pseudonimização é o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro.

CAPÍTULO IX

DAS RESPONSABILIDADES

Art. 14º As responsabilidades para a Gestão da Segurança da Informação são atribuídas da seguinte forma:

I - Comitê de Governança Digital (CGD): aprova a Política de Segurança da Informação e suas revisões, designa os proprietários da informação se necessário, e toma as decisões administravas referentes aos casos de descumprimento da política e/ou de suas normas, encaminhados pelo Comitê de Segurança da Informação.

II - Comitê de Segurança da Informação (CSI): grupo de pessoas cuja composição, forma de deliberação e periodicidade de reuniões é normatizada em portaria específica, sendo responsável por analisar e propor medidas para efetiva aplicação, disseminação e aprimoramento da Política de Segurança da Informação e por dirimir dúvidas e a propriedade dos ativos de informação.

III- Diretoria de Tecnologia da Informação (DTI): regulamenta e operacionaliza as normas provenientes da Política de Segurança da Informação, o que inclui manutenção e uso dos recursos computacionais, implantação e manutenção de Data Center, controle de acesso a serviços de rede, gerenciamento de credenciais de acesso aos sistemas institucionais, Plano de Continuidade do Negócio, estratégias de backup, Acordos de Nível de Serviço, manutenção do inventário de ativos de tecnologia da informação, proteção contra invasões e malwares, homologação, instalação, remoção e atualização de softwares, controle de dispositivos conectados à rede de dados institucional, implantação, configuração e monitoramento do desempenho de ativos de rede, e definição de processos de resolução de incidentes.

IV- Pró-reitoria de Gestão de Pessoas (PROGEP): executa as ações de treinamento e desenvolvimento referentes à Segurança da Informação. Informa a área de TI dos

desligamentos e afastamentos de servidores do quadro funcional do Instituto para a devida revogação de acesso aos sistemas institucionais.

V- Coordenadoria de Comunicação Social (CCS): executa as atividades relacionadas à comunicação institucional, divulgando e disseminando as orientações emanadas pela Política de Segurança da Informação.

VI - Gestores Administrativos: multiplicam e catalisam os princípios de segurança; autorizam concessão, transferência e revogação de acessos; responde conjuntamente pelas ações realizadas por seus subordinados; conscientizam os usuários sob sua supervisão em relação aos conceitos e às práticas de SI; incorporam aos processos de trabalho de sua unidade, ou de sua área, práticas inerentes à SI; tomam as medidas administravas necessárias para que sejam aplicadas ações corretivas nos casos de comprometimento da SI por parte dos usuários sob sua supervisão.

VII - Usuários: observam e acatam as recomendações para a utilização segura dos recursos de tecnologia da informação e, em caso de dúvidas ou problemas relacionados com sites ou e-mails suspeitos, extravio de informações, danos e roubo de equipamentos sob sua custódia, contatam a DTI para tomada de ações cabíveis; protegem os ativos de informação do IFSul, incluindo informação, evitando perda ou modificação de dados, software e hardware; observam restrições em relação a cópias e divulgação de informações, e uso dos acordos de confidencialidade; observam restrições em relação à manutenção e instalação de software e hardware; atende à política de controle de acesso do IFSul; relatam incidentes de segurança da informação e violação da segurança; atendem aos princípios e diretrizes contidos nesta POSIN, incluindo normas e procedimentos complementares destinados à SI; são responsáveis por todos os atos praticados com suas identificações (login, crachá, carimbo, e-mail, assinatura digital, etc.).

VIII – Encarregado de dados (DPO): Na definição do artigo 5º, inciso VIII, da LGPD, o encarregado é a pessoa indicada pelo controlador Institucional para atuar como canal de comunicação entre o controlador, os titulares dos dados pessoais e a Autoridade Nacional de Proteção de Dados (ANPD).

A ANPD poderá estabelecer normas complementares sobre a definição e as atribuições do encarregado, inclusive hipóteses de dispensa da necessidade de sua indicação, conforme a natureza e o porte da entidade ou o volume de operações de tratamento de dados.

CAPÍTULO X

DO ACESSO, PROTEÇÃO E GUARDA DA INFORMAÇÃO

Art. 15º O acesso à informação dentro da rede do IFSul deve ser realizado através de credenciais de acesso obtidos por meio de abertura de chamado na central de serviços no Sistema Unificado de Administração Pública (SUAP).

Art. 16º Toda e qualquer informação gerada, adquirida, utilizada ou armazenada pelo IFSul é considerada seu patrimônio e deve ser protegida.

Parágrafo único. Qualquer falha na segurança da informação, identificada por qualquer usuário, deve ser imediatamente comunicada ao CSI para avaliação e determinação das ações que se fizerem necessárias.

Art. 17º Todos os usuários que manipulem ou tenham acesso a informações identificadas como reservadas sob custódia ou propriedade do IFSul devem garantir a confidencialidade e o sigilo destas informações, adotando comportamento seguro e discreto, evitando expô-las em ambientes sociais e particulares, ou através de impressão, transmissão/compartilhamento digital e transporte físico para fora das instalações do IFSul sem autorização formal.

Art. 18º As violações de segurança devem ser comunicadas e registradas para tomada de ações imediatas de caráter corretivo, legal e de auditoria, além de compor base de conhecimento sobre incidentes de segurança da informação para posterior análise com o propósito de ajustar as medidas preventivas.

CAPÍTULO XII
DA UTILIZAÇÃO DOS RECURSOS COMPUTACIONAIS

Art. 19º Os recursos computacionais disponibilizados pelo IFSul são fornecidos com o propósito único de garantir o bom desempenho das atividades do IFSul, sendo vedado aos usuários: o uso desses recursos para constranger, assediar, ofender, caluniar, ameaçar ou causar prejuízos a qualquer pessoa física ou jurídica; armazenar, transmitir ou compartilhar arquivos pessoais ou não relacionados às suas atividades nos recursos corporativos; e quaisquer outras atividades que contrariem os objetivos institucionais do IFSul.

Art. 20º Os acessos à rede de dados do IFSul devem ser monitorados e controlados para todos os tipos de protocolos de conexão, devendo os usuários de serviços de rede ser identificados e ter acesso apenas às informações e aos recursos necessários ao desempenho de suas atividades.

Art. 21º Todos os ativos de informação do parque computacional devem ser inventariados, incluindo-se dispositivos móveis como **notebooks**, **tablets** e **smartphones**, quando pertencentes ao IFSul, com identificação patrimonial e de seus responsáveis, bem como a definição de suas configurações, manutenções e documentações pertinentes.

Parágrafo único. Todo o ativo de informação deve ser protegido e conservado, de forma a preservar os seus componentes internos, externos e acessórios.

CAPÍTULO XIII
DA SEGURANÇA FÍSICA E DO AMBIENTE E DE RECURSOS HUMANOS

Art. 22º Tendo em vista a necessidade de se garantir a segurança física e do ambiente, bem como a segurança de recursos humanos, o IFSul estabelecerá controles, visando a:

I- Prevenir o acesso físico indevido e sem autorização, bem como danos e interferências com as instalações e informações do IFSul; e

II- Assegurar que os usuários, prestadores de serviço e terceiros entendam suas responsabilidades e assinem acordos sobre seus papéis e responsabilidades pela segurança da informação, com a finalidade de reduzir os riscos de burla, erros humanos, furto, roubo, apropriação indébita, fraude, ou uso indevido dos ativos de informações do IFSul.

III. Os ambientes onde estão instalados os ativos de missão crítica e armazenamento de dados devem ter acesso controlado, a DTI e CSI concederão os privilégios de acesso aos usuários, e classificarão as áreas físicas protegidas contra o acesso de pessoas não autorizadas.

IV. Para os sistemas de missão crítica, deverão ser mantidos serviços ou utilizados equipamentos que disponham de recursos de redundância de processamento, armazenamento de dados, sistemas elétricos, etc., bem como, controle de corrente elétrica (rede estabilizada), temperatura, climatização e acesso físico restrito.

V. Os ativos computacionais tipo servidores de redes, onde se encontram os sistemas de missão crítica, devem estar em sala segura contra problemas de segurança física (condições ambientais adversas, desastres naturais, incêndios, acesso indevido, etc.).

VI. Cabe ao responsável zelar pelo ativo físico e/ou lógico outorgado pela instituição.

Art. 23º Os serviços de rede no ambiente do IFSul também constituem ativos passíveis de inventário, documentação e auditoria, devendo estes procedimentos serem realizados conforme procedimentos indicados nesta política e normas complementares elaboradas pela CSI:

I. Sempre que possível registar e tratar os logs dos sistemas e dispositivos para análise, diagnósticos e ações de correção.

II. Registar o fluxo de entrada e saída do tráfego da rede para análise do caminho, protocolos e volume dos dados institucionais que circulam pela intranet e internet.

III. Registrar as métricas dos ativos de rede e sistemas, para identificar as cargas e desempenho dos ativos de informação.

IV. Sempre que possível, implementar e manter ativo os serviços de auditoria dos ativos de informação;

V. O CSI especificara em norma complementar o detalhamento destes procedimentos e outros que se fizerem necessário para manter a segurança da informação no âmbito da rede física e lógica do IFSul.

Art. 24º Equipamentos particulares e/ou privados, como computadores ou quaisquer dispositivos que possam armazenar e/ou processar dados, não devem ser usados para armazenar e/ou processar informações que sejam classificadas como sensíveis para a atividade do IFSul, sem prévia autorização expressa do custodiante dos dados.

CAPÍTULO XIV
DA GESTÂO DE CONTINUIDADE DE NEGÓCIO

Art. 25º Os procedimentos que garantam a continuidade e a recuperação do fluxo de informações devem ser mantidos, observando-se as classificações de disponibilidades requeridas, de forma a não permitir a interrupção das atividades de negócios e proteger os processos críticos contra falhas e danos, que atenderão aos seguintes objetivos:

I- Avaliação em regime emergencial das consequências de desastres, falhas de segurança e perda de serviços.

II - Contingência e recuperação do funcionamento normal dentro de períodos de tempo determinados.

III - Recuperação tempestiva das operações consideradas vitais.

CAPÍTULO XV

DA AUDITORIA E CONFORMIDADE

Art. 26º Devem ser adotados procedimentos apropriados para garantir a conformidade e o respeito às restrições legais quanto ao uso e disseminação de informações protegidas por leis, tais como: dados pessoais relativos à intimidade, à vida privada, à honra e à imagem, de propriedade intelectual, direitos autorais, segredos comerciais e de Industria, patentes e marcas registradas, ou aquelas classificadas como reservadas.

Art. 27º Os processos de aquisição de bens e serviços, especialmente dos ativos de informação, devem estar em conformidade com esta POSNI.

Art. 28º Os sistemas de informações, além de disponibilizar os registros em prazos e formatos aceitáveis, devem protegê-los contra perda, destruição e falsificação, visando à salvaguarda dos dados.

CAPÍTULO XVI

DA GESTAO DE RISCOS DE SEGURANÇA DA INFORMAÇAO

Art. 29º O CSI buscará identificar ameaças e vulnerabilidades que poderão expor o IFSUL, para isso serão avaliadas as infraestruturas local e de nuvem.

Art.30º Na análise de risco de cada solução serão identificadas as ameaças e vulnerabilidades em potencial à segurança da Informação e sua probabilidade aproximada, será observado o contexto tecnológico e não tecnológico relacionado e identificados quais os requisitos de segurança que existem ou que deveriam existir para proteger o ativo.

Art. 31º A gestão de vulnerabilidades deverá ser de fluxo contínuo, visto que as redes de computadores, aplicações web, banco de dados são elementos dinâmicos, as vulnerabilidades podem surgir diariamente devido a configurações indevidas e atualizações, diante deste dinamismo de vulnerabilidade se faz necessário adotar medidas de testagem regular das vulnerabilidades de rede. A análise contínua é um componente crítico para identificar e mitigar riscos de segurança da informação.

Art. 36. Realizar backup imediatamente em casos de ataques cibernéticos, para isso é importante ter um software que permitem fazer backup de forma rápida e automática, o backup é, antes de tudo, uma filosofia de trabalho que exige disciplina e constância.

Art. 32º Em casos de invasão será realizada a coleta das evidências do crime cibernético ou roubo de dados que venha a acometer a instituição, deverão ser salvos os arquivos, e-mails, capturas de telas, e qualquer outro material que comprove o crime.

Art. 33º Considerando que o usuário (lado humano), conhecido como camada 8, é o vetor de comunicação mais tolerável da cadeia de ataque, suscetível as técnicas de engenharia social, se faz necessário desenvolver uma cultura de segurança da informação com campanhas, manter um programa de conscientização e consequentemente aumentar sua maturidade da comunidade acadêmica.

Art. 34º O Gerenciamento de Risco um processo contínuo e iterativo e suas atividades e fases conterá necessariamente uma matriz de probabilidade e impacto, compreendendo as ameaças, vulnerabilidades e probabilidade de ocorrências, a classificação dos riscos e alternativas de mitigação.

Art. 35º A instituição deverá homologar os softwares que poderão ser instalados nos equipamentos da instituição, os mesmos poderão constar em planilha editável, compartilha entre todos os profissionais de TIC da instituição, qualquer destes, poderão homologar e incluir novos softwares na lista, identificando o nome do responsável, o nome software e tipo de licença, em caso de software proprietário que necessite de licença paga, deverá indicar se a validação foi adquirida e o tempo de permissão de uso, informar o campus e ou setor.

Art. 36º A qualquer tempo, a DTI ou CSI poderá revogar a homologação se identificado vulnerabilidade insanável e que fragilize a segurança da informação, nesse caso é obrigatório a desinstalação ou isolamento do dispositivo, de forma que não comprometa outros ativos de informação e em última instância a CSI poderá permitir o uso mesmo colocando a segurança em risco.

Art. 37º A instalação de software em equipamentos da instituição deve ser previamente autorizada pelo setor de TI do Campus, DTI ou Comitê de Governança Digital.

Art. 38º É vedada a utilização e/ou instalação de software que possa de qualquer forma ferir esta política de segurança, bem como direitos autorais, de propriedade intelectual ou quaisquer legislações vigentes, em caso de ilícito o colaborador que der causa arcará com as responsabilidades.

Art. 39º É terminantemente proibido a utilizar software proprietário sem a devida licença e/ou utilizar de meios e mecanismos fraudulento de licenciamento (crack) e outros.

CAPÍTULO XVII
DA AVALIAÇÃO E DA REGULAMENTAÇÃO

Art. 40º O cumprimento desta POSIN deve ser avaliado periodicamente, de acordo com os critérios do CSI.

Art. 41º Fica a DTI autorizada a regulamentar e submeter à Reitoria do IFSul, para aprovação, os procedimentos necessários para a aplicação das disposições estabelecidas nesta POSIN, que estarão consubstanciadas na norma complementar que regulamenta o uso de recursos computacionais, de sistemas de informação, de acesso lógico, de rede de comunicações e de continuidade do negócio do IFSul.

CAPÍTULO XIII

DISPOSIÇÕES FINAIS

Art. 42º A Política de Segurança da Informação será revisada e atualizada anualmente, ou sempre que ocorrerem eventos ou fatores relevantes que exijam sua revisão imediata.

Art. 43º É vedada qualquer ação que não esteja explicitamente permitida na POSIN do IFSul ou que não tenha sido previamente autorizada pelo CSI.

Art. 44º 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. 45º Casos omissos serão analisados e deliberados pelo CSI do IFSul.

Art. 46º Esta Resolução entrará em vigor na data de sua assinatura.

Documento Digitalizado Público

Política de Segurança da Informação do IFSul

Assunto: Política de Segurança da Informação do IFSul
Assinado por: -
Tipo do Documento: Documento Genérico
Situação: Finalizado
Nível de Acesso: Público
Tipo do Conferência: Cópia Simples