MINISTÉRIO DA EDUCAÇÃO
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA FARROUPILHA

Política da Segurança da Informação – PSI.

CAPÍTULO I
DISPOSIÇÕES GERAIS

Art. 1º. Este documento institui a Política de Segurança da Informação (PSI) do Instituto Federal Farroupilha (IFFar) e se aplica a todas as unidades regimentais da Instituição.

§ 1º. A PSI dispõe sobre as orientações para gestão de segurança da informação, que devem ser observadas e implementadas pelo IFFar, com a finalidade de assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação, em âmbito Institucional.

§ 2º. A PSI do IFFar foi desenvolvida com base nas recomendações da Norma NBR ISO/IEC 27002:2022 - Segurança da Informação, Segurança Cibernética e Proteção da Privacidade - Controles de Segurança da Informações e da Norma NBR ISO/IEC 27001:2022 - Segurança da informação, segurança cibernética e proteção à privacidade - Sistemas de gestão da segurança da informação – Requisitos, além de estar embasada na Instrução Normativa nº 1, de 27/05/2020, que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal e no Decreto nº 9.637 de 26/12/2018, que institui a Politica Nacional de Segurança da Informação nos órgãos e entidades da Administração Pública Federal.

CAPÍTULO II
DO ESCOPO E ABRANGÊNCIA

Art. 2º. Para os fins do disposto nesta PSI, a segurança da informação abrange: a defesa cibernética, a segurança física, a proteção de dados organizacionais e as ações destinadas a assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação.

Parágrafo Único. A PSI é composta por diretrizes, normas, procedimentos e responsabilidades adequadas para manuseio, tratamento, controle e proteção das informações mantidas pelo IFFar, sendo válida para todos os usuários de informações da Instituição.

Art. 3º As orientações contidas na PSI deverão ser seguidas e cumpridas por todos os servidores, alunos, estagiários, consultores externos e prestadores de serviço que exerçam atividades, ou que possuam acesso a dados ou informações, no ambiente do IFFar.

CAPÍTULO III
DOS CONCEITOS E DEFINIÇÕES

Art. 4º. Para fins de uniformidade dos procedimentos contidos nesta PSI, devem ser 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, materiais 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, nobreaks e quaisquer outros bens. Qualquer bem, tangível ou intangível, que tenha valor para o IFFar.

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

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 - Política de Privacidade e Proteção de Dados.

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.

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 por 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 IFFar.

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, colaboradores, alunos e pais, 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 IFFar, de acordo com o estabelecido em normas específicas - Política de Privacidade e Proteção de Dados.
XVIII - Usuários: são as pessoas que utilizam os recursos e serviços de Tecnologia da Informação tecnologia da informação (TI) disponibilizados pelo IFFar, podendo ser servidor de cargo efetivo ou temporário, cedido ou de cooperação técnica, oriundo de outro órgão, alunos da Instituição, bem como seus pais ou responsáveis, prestador de serviço tercerizado, convidados ou quaisquer outros com autorização prévia do IFFar.

CAPÍTULO IV
DAS REFERÊNCIAS LEGAIS E NORMATIVAS

Art. 5º. As diretrizes básicas da Política de Segurança da Informação do IFFar devem atender às seguintes referências legais e normativas, além das citadas no Art. 1º, parágrafo 2, sem prejuízo das demais normas em vigor:
I - Resolução SE/GSI nº 1, de 11 de setembro de 2019, que aprova o Regimento Interno do Comitê Gestor de Segurança da Informação.
II - Portaria GSI/PR nº 93, de 26 de setembro de 2019, que aprova o Glossário de Segurança da Informação.
III - Decreto nº. 10.222, de 5 de fevereiro de 2020, que aprova a Estratégia Nacional de Segurança Cibernética.
IV - Lei nº. 12.527, de 18 de novembro de 2011, que dispõe sobre o acesso à informação pública.
V - Decreto no 7.724, de 16 de maio de 2012, que regulamenta o acesso à informação pública.
VI - 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.
VII - Lei nº. 13.709, de 14 de agosto de 2018 (LGPD), que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

CAPÍTULO V
DOS PRINCÍPIOS

Art. 6º. O IFFar atua em conformidade com os procedimentos estabelecidos nesta PSI, observando os seguintes princípios:
I - Autenticidade;
II - Ciência;
III - Confidencialidade;
IV - Criticidade;
V - Disponibilidade;
VI - Ética;
VII - Integridade;
VIII - Legalidade;
IX - Não-Repúdio;
X - Proporcionalidade;
XI - Responsabilidade.

Art. 7º. O IFFar exonera-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 usuários pertencem ao IFFar. As exceções devem ser formalizadas explicitamente entre as partes.

§ 2º. Todos os ativos de informação do IFFar, incluindo os recursos computacionais, devem ser utilizados de forma ética, responsável e consciente, aplicados no alcance dos objetivos institucionais do IFFar.
§ 3º. Os sistemas informacionais do IFFar serão utilizados mediante controle de acesso, gerenciados e monitorados com apoio de ferramentas tecnológicas adequadas, com processos de negócio suficientemente definidos para assegurar a devida proteção dos ativos de informação e da infraestrutura computacional da Instituição.
§ 4º. O usuário é individualmente responsável pela segurança das informações dentro do IFFar, principalmente daquelas que estejam sob sua responsabilidade.
§ 5º. É recomendado constar em todos os contratos celebrados pelo IFFar, clausula 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 VI
DAS DIRETRIZES

Art. 8º. As diretrizes desta PSI devem ser amplamente divulgadas nos setores do IFFar, inclusive em sala de aula e site institucional, garantindo que todos tenham acesso e adquiram consciência sobre as orientações de segurança da informação.
I - O IFFar deve instituir formalmente um responsável pela segurança da informação na organização, conforme orientação contida na NBR ISO/IEC 27002:2022.
II - A Gestão de Segurança da Informação do IFFar 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 IFFar 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 IFFar 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 IFFar 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 institucionais.
VIII - Deve ser estabelecido um processo de Gestão de Riscos de Segurança da Informação, gerido pelo Time de Respostas a Incidentes, 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 IFFar, 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 PSI deve ser avaliado, periodicamente, pela alta administração, em conformidade com normas complementares, manuais de procedimentos e legislação, buscando a certificação do atendimento dos requisitos de segurança da informação.

XI - Devem ser instituídas normas complementares à PSI, 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 IFFar. 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 e monitoradas, de forma a manter o nível adequado da segurança da informação e detectar atividades não autorizadas.
XIII - Os ativos da organização devem ser protegidos contra acesso físico não autorizado, danos, perdas, furto e interferência. A proteção deve estar alinhada aos riscos identificados.

CAPÍTULO VII
DAS RESPONSABILIDADES

Art. 9º. As responsabilidades para a Gestão da Segurança da Informação são atribuídas da seguinte forma:
I - Comitê Gestor de Tecnologia da Informação (CGTI): realiza a aprovação da Política de Segurança da Informação e suas revisões, bem como a tomada de decisões administrativas 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): responsável por analisar e propor medidas para efetiva aplicação, disseminação e aprimoramento da Política de Segurança da 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 – Secretaria de Comunicação Social (SECOM): executa as atividades relacionadas à comunicação institucional, divulgando e disseminando as orientações emanadas pela Política de Segurança da Informação.
V - Gestores Administrativos: multiplicam e catalisam os princípios de segurança; autorizam concessão, transferência e revogação de acessos; respondem 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 administrativas necessárias para que sejam aplicadas ações corretivas nos casos de comprometimento da SI por parte dos usuários sob sua supervisão.
VI - 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 IFFar, 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; atendem à política de controle de acesso do IFFar; relatam incidentes de segurança da informação e violação da segurança; atendem aos princípios e diretrizes contidos nesta PSI, 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.).

VII – Encarregado de proteção de dados (DPO): segundo a Lei Geral de Proteção de Dados (LGPD), o encarregado é a pessoa indicada pelo controlador Institucional (quem define os parâmetros do processo de tratamento de dados, tomando as decisões do que deve ser feito) para atuar como canal de comunicação entre o controlador, os titulares dos dados pessoais e a Autoridade Nacional de Proteção de Dados (ANPD).

CAPÍTULO VIII
DO TRATAMENTO DE DADOS PESSOAIS

Art. 10º. Tratamento de dados é toda operação realizada com dados pessoais: acesso, armazenamento, arquivamento, avaliação, classificação, coleta, comunicação, controle, difusão, distribuição, eliminação, extração, modificação, processamento, produção, recepção, reprodução, transferência, transmissão e utilização.

Parágrafo único. O tratamento de dados pessoais obedecerá ao regramento da LGPD (Lei nº 13.709, de 14 de agosto de 2018) e somente poderá ser realizado nas seguintes hipóteses:

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

II. Mediante o consentimento do titular dos dados pessoais.

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

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

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 dos dados.

II. Forma e duração do tratamento dos dados.

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 dos dados.

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

CAPÍTULO IX
DO ACESSO, PROTEÇÃO E GUARDA DA INFORMAÇÃO

Art. 12º. O acesso à informação, dentro da rede do IFFar, deve ser realizado através de credenciais de acesso obtidas por meio de abertura de chamado no Sistema de Suporte Institucional (GLPI), através do endereço eletrônico https://suporte.iffarroupilha.edu.br.

Art. 13º. Toda e qualquer informação gerada, adquirida, utilizada ou armazenada pelo IFFar é considerada seu patrimônio e deve ser protegida.

Parágrafo único. Qualquer falha na segurança da informação, identificada por usuário, deve ser imediatamente comunicada à DTI e esta deve reportar a falha ao CGSI, para avaliação e determinação das ações necessárias.

Art. 14º. Todos os usuários que manipulem ou tenham acesso a informações identificadas como reservadas, sob custódia ou propriedade do IFFar, 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 IFFar, sem autorização formal.

Art. 15º. 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 X
DA UTILIZAÇÃO DOS RECURSOS COMPUTACIONAIS

Art. 16º. Os recursos computacionais disponibilizados pelo IFFar são fornecidos como propósito único de garantir o bom desempenho das atividades da Instituição, 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 IFFar.

Art. 17º. Os acessos à rede de dados do IFFar devem ser monitorados e controlados para todos os tipos de protocolos de conexão, identificando os usuários de serviços de rede e oferecendo acesso apenas às informações e recursos necessários ao desempenho de suas atividades.

Art. 18º. Todos os ativos de informação do parque computacional devem ser inventariados, incluindo dispositivos móveis (notebooks, tablets e smartphones), quando pertencentes ao IFFar, com identificação patrimonial e de seus responsáveis, bem como a definição de suas configurações, manutenções e documentações pertinentes.

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

Art. 19º. Tendo em vista a necessidade de garantir a segurança física e do ambiente, bem como a segurança de recursos humanos, o IFFar estabelecerá controles, visando:
I - Prevenir o acesso físico indevido e sem autorização, bem como danos e interferências com as instalações e informações do IFFar.
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 erros humanos, furto, roubo, apropriação indébita, fraude, ou uso indevido dos ativos de informações do IFFar.
III. Os ambientes onde estão instalados os ativos de missão crítica, armazenamento de dados, servidores de redes devem ter acesso controlado. A DTI, CGSI e Coordenação de Tecnologia da Informação (CTI) dos campi 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, bem como controle de corrente elétrica (rede estabilizada), climatização e acesso físico restrito.
Art. 20º. Os serviços de rede no ambiente do IFFar também constituem ativos passíveis de inventário, documentação e auditoria, devendo estes procedimentos serem realizados conforme procedimentos indicados nesta política e normas complementares, elaboradas pela CGSI.

Art. 21º. 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 IFFar, sem prévia autorização expressa do detentor dos dados, conforme Política de Privacidade e Proteção de Dados.

CAPÍTULO XII
DA GESTÃO DE CONTINUIDADE DE NEGÓCIO

Art. 22º. Com o objetivo de evitar situações de interrupção, manter as atividades de negócios e proteger os processos críticos e sistemas de informação do IFFar, o CGSI, com a participação da DTI e CGTI, deverá manter um Plano de Contingência e Continuidade dos Serviços de Tecnologia da Informação, com objetivo de garantir a recuperação rápida e eficaz após uma interrupção.

Parágrafo Único. O PGCN deve incluir:
I - Identificação das atividades críticas do IFFar.
II - Avaliação de riscos e ameaças potenciais.
III - Definição de estratégias de recuperação.
IV - Implementação de medidas de contingência.
V - Treinamento dos envolvidos.
VI - Realização de testes regulares.

CAPÍTULO XIII
DA AUDITORIA E CONFORMIDADE

Art. 22º. O CGSI deverá propor normas complementares ao CGTI, a fim de manter registros, como mecanismo de auditoria que possibilite o rastreamento, acompanhamento, controle e verificação de acesso aos serviços, sistemas de informação e rede interna, em conformidade com essas normas.

Art. 23º 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 indústria, patentes e marcas registradas, ou aquelas classificadas como reservadas.

Art. 24º. Deve ser realizada, periodicamente, a verificação de conformidade das práticas de segurança da informação do IFFar, desta PSI e de suas normas e procedimentos complementares, bem como com a legislação específica de segurança da informação.
Parágrafo Único. A verificação de conformidade deve também ser realizada nos contratos, convênios, acordos de cooperação e outros instrumentos do mesmo gênero, celebrados pelo IFFar.

CAPÍTULO XIV
DA GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO

Art. 25º. 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 implementação de controles para a identificação e o tratamento de possíveis falhas de segurança.
§ 1º O CGSI deve definir e adotar processo contínuo de Gestão de Riscos de Segurança da Informação (GRSI), com a contribuição e homologação do CGTI.
§ 2º. O processo de GRSI deverá ser revisto periodicamente pelo CGSI e CGTI, a fim de aperfeiçoar e agir proativamente contra riscos advindos de novas tecnologias e ameaças, objetivando a constante elaboração de planos de ação apropriados para a proteção dos seus ativos de informação.
§ 3º. É função do CGSI a criação e atualização periódica do Plano de Tratamento de Riscos, com a participação do CGTI.
§ 4.º É função do CGSI identificar ameaças e vulnerabilidades de segurança de informação no âmbito do IFFar, nas infraestruturas local e de nuvem.

Art. 26º. 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. 27º. A gestão de vulnerabilidades deverá ser de fluxo contínuo, visto que as redes de computadores, aplicações web, banco de dados são elementos dinâmicos e as vulnerabilidades podem surgir devido a configurações incorretas e atualizações.
Parágrafo Único. Em casos de invasão cibernética deve ser realizada a coleta das evidências do crime cibernético ou roubo de dados da Instituição, coletando arquivos, e-mails, capturas de telas, e qualquer outro material que comprove o crime, segundo Plano de Gestão de Riscos e Plano de Contingência e Continuidade dos Serviços de Tecnologia da Informação.

Art. 28º. A cultura de segurança da informação deve ser desenvolvida por meio de campanhas e programas de conscientização, com objetivo de aumentar a maturidade tecnológica dos usuários, os tornando menos vulneráveis e suscetíveis a ataques cibernéticos.

Art. 29º. 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. 30º. É proibido utilizar software proprietário sem a devida licença e/ou utilizar meios e mecanismos fraudulentos de licenciamento, entre outros.

CAPÍTULO XV
DA AVALIAÇÃO E DA REGULAMENTAÇÃO

Art. 31º. O cumprimento desta PSI deve ser avaliado periodicamente, de acordo com os critérios do CGSI.

Art. 32º. Fica a DTI autorizada a regulamentar e submeter aos colegiados e conselhos superiores do IFFar, para aprovação, os procedimentos necessários para a aplicação das disposições estabelecidas nesta PSI, 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 IFFar.

CAPÍTULO XVI
DAS PENALIDADES

Art. 33º. O descumprimento ou violação das disposições constantes nesta Política de Segurança da Informação, 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. 34º. Os casos omissos serão analisados e deliberados pelo CGSI do IFFar.

CAPÍTULO XVII
DISPOSIÇÕES FINAIS

Art. 35º. Esta Política de Segurança da Informação será revisada e atualizada anualmente, ou na ocorrência de eventos ou fatores relevantes que exijam sua revisão imediata.