MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO TOCANTINS
REITORIA

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Estabelece a Política de Segurança da Informação (PSI) no âmbito do Instituto Federal de Educação, Ciência e Tecnologia do Tocantins (IFTO).

O REITOR DO INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO TOCANTINS, nomeado pelo Decreto Presidencial de 3 de abril de 2018, publicado no Diário Oficial da União de 4 de abril de 2018, seção 2, no uso de suas atribuições legais e regimentais, e com base no inciso IX do art. 61, art. 76-A e § 4º do art. 98 da Lei nº 8.112, de 11 de dezembro de 1990, no Decreto nº 6.114, de 15 de maio de 2007, e na Portaria MEC nº 1.084, de 2 de setembro de 2008, publicada no DOU de 3 de setembro de 2008, resolve estabelecer a Política de Segurança da Informação do IFTO.

CAPÍTULO I
DO ESCOPO

Art. 1° A Política de Segurança da Informação (PSI) tem o objetivo de declarar o comprometimento da alta administração com vistas a estabelecer diretrizes estratégicas, responsabilidades, competências, apoio e subsídios para implementar a gestão da segurança da informação no âmbito do IFTO.

Parágrafo único. Esta política será complementada por: normas, processos, metodologias, procedimentos e controles a serem adotados para a gestão de segurança da informação e privacidade de dados, considerando os requisitos legais, processos organizacionais, planos institucionais e estrutura organizacional do IFTO.

Art. 2° Esta PSI abrange a seguinte estrutura de privacidade e gestão de segurança da informação:

I - segurança cibernética;

II - defesa cibernética;

III - segurança física;

IV - proteção de dados organizacionais; e

V - ações destinadas a assegurar a disponibilidade, integridade, a confidencialidade e a autenticidade da informação.

CAPÍTULO II
DAS REFERÊNCIAS SOBRE SEGURANÇA DA INFORMAÇÃO

Art. 3º Para o planejamento da gestão da segurança da informação, cabe ao IFTO observar, sem prejuízo das demais normas em vigor:

I - Decreto nº 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação;

II - Resolução SE/GSI nº 1, de 11 de setembro de 2019, que aprova o Regimento Interno do Comitê Gestor de Segurança da Informação;

III - Portaria GSI/PR nº 93, de 26 de setembro de 2019, que aprova o Glossário de Segurança da Informação;

IV - Decreto nº 10.222, de 5 de fevereiro de 2020, que aprova a Estratégia Nacional de Segurança Cibernética;

V - Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020 que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal;

VI - Instrução Normativa GSI/PR nº 3, de 28 de maio de 2021 que dispõe sobre os processos relacionados à gestão de segurança da informação nos órgãos e nas entidades da administração pública federal;

VII - 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 , 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;

VIII - Portaria SGD/MGI nº 852, de 28 de março de 2023, que dispõe o Programa de Privacidade e Segurança da Informação.

IX - demais leis, decretos, resoluções, portarias e instruções normativas relacionadas à segurança da informação, publicadas pelo Gabinete de Segurança Institucional da Presidência da República.

CAPÍTULO III
DOS CONCEITOS E DEFINIÇÕES

Art. 4° Para fins de compreensão dos termos utilizados nesta PSI serão utilizados os seguintes conceitos e definições:

I - ameaça: conjunto de fatores externos com o potencial de causar dano para um sistema ou organização;

II - alta administração: representa o mais alto nível estratégico e decisório de um órgão ou entidade, seja ela parte da administração pública federal direta ou indireta;

III - atividade: ação ou conjunto de ações executadas por um órgão ou entidade, ou em seu nome, que produzem ou suportem um ou mais produtos ou serviços;

IV - ativo: tudo que tenha valor para a organização, material ou não;

V - ativos 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;

VI - *backup/cópia de segurança:* conjunto de procedimentos que permitem salvaguardar os dados de um sistema computacional, garantindo guarda, proteção e recuperação. Tem a fidelidade ao original assegurada. Esse termo também é utilizado para identificar a mídia em que a cópia é realizada;

VII - banco de dados: coleção de dados inter-relacionados, representando informações sobre um domínio específico. São coleções organizadas de dados que se relacionam, a fim de criar algum sentido (informação) e de dar mais eficiência durante uma consulta ou a geração de informações ou conhecimento;

VIII - comitê de segurança da informação (CSI): grupo de pessoas com a responsabilidade de assessorar a implementação das ações de segurança da informação no âmbito do órgão ou entidade da administração pública federal;

IX - computação em nuvem: modelo de fornecimento e entrega de tecnologia de informação que permite acesso conveniente e sob demanda a um conjunto de recursos computacionais configuráveis, sendo que tais recursos podem ser provisionados e liberados com mínimo gerenciamento ou interação com o provedor do serviço de nuvem;

X - controle de acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso ao uso de recursos físicos ou computacionais. Via de regra, requer procedimentos de autenticação;

XI - controle: forma de gerenciar o risco, incluindo políticas, procedimentos, diretrizes, práticas ou estrutura organizacionais, que podem ser de natureza administrativa, técnica, de gestão ou legal;

XII - controles de segurança: certificado que autoriza uma pessoa natural para o tratamento de informação classificada;

XIII - criptografia: arte de proteção da informação, por meio de sua transformação em um texto cifrado (criptografado), com o uso de uma chave de cifragem e de procedimentos computacionais previamente estabelecidos, a fim de que somente o(s) possuidor(es) da chave de decifragem possa(m) reverter o texto criptografado de volta ao original (texto pleno). A chave de decifragem pode ser igual (criptografia simétrica) ou diferente (criptografia assimétrica) da chave de cifragem;

XIV - CTIR GOV - Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo, subordinado ao Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República;

XV - descarte: eliminação correta de informações, documentos, mídias e acervos digitais;

XVI - diretriz: descrição que orienta o que deve ser feito e como, para se alcançarem os objetivos estabelecidos nas políticas;

XVII - documento: unidade de registro de informações, qualquer que seja o suporte ou o formato;

XVIII - e-mail: sigla de correio eletrônico (*electronic mail*);

XIX - eliminação: exclusão de dado ou conjunto de dados, armazenados em banco de dados, independentemente do procedimento empregado;

XX - equipe de tratamento e resposta a incidentes cibernéticos (ETIR): grupo de agentes públicos com a responsabilidade de prestar serviços relacionados à segurança cibernética para o órgão ou a entidade da administração pública federal, em observância à política de segurança da informação e aos processos de gestão de riscos de segurança da informação do órgão ou da entidade;

XXI - evento: qualquer mudança de estado que tem importância para a gestão de um item de configuração ou serviço de tecnologia da informação. Em outras palavras, qualquer ocorrência dentro do escopo de tecnologia da informação que tenha relevância para a gestão dos serviços entregues ao cliente;

XXII - evento de segurança: qualquer ocorrência identificada em um sistema, serviço ou rede, que indique uma possível falha da política de segurança, falha das salvaguardas ou mesmo uma situação até então desconhecida, que possa se tornar relevante em termos de segurança;

XXIII - firewall: ferramenta para evitar acesso não autorizado, tanto na origem quanto no destino, a uma ou mais redes. Podem ser implementados por meio de *hardware* ou *software*, ou por meio de ambos. Cada mensagem que entra ou sai da rede passa pelo *firewall*, que a examina a fim de determinar se atende ou não os critérios de segurança especificados;

XXIV - gestão de continuidade de negócios em segurança da informação: processo que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio, caso estas ameaças se concretizem. Esse processo fornece uma estrutura para que se desenvolva uma resiliência organizacional que seja capaz de responder efetivamente e salvaguardar os interesses das partes interessadas, a reputação, a marca da organização e suas atividades de valor agregado;

XXV - gestão de segurança da informação: processo que visa integrar atividades de gestão de riscos, gestão de continuidade do negócio, tratamento de incidentes, tratamento da informação, conformidade, credenciamento, segurança cibernética, segurança física, segurança lógica, segurança orgânica e organizacional, aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto, à tecnologia da informação;

XXVI - incidente: interrupção não planejada ou redução da qualidade de um serviço, ou seja, ocorrência, ação ou omissão, que tenha permitido, ou possa vir a permitir, acesso não autorizado, interrupção ou mudança nas operações (inclusive pela tomada de controle), destruição, dano, deleção ou mudança da informação protegida, remoção ou limitação de uso da informação protegida ou ainda a apropriação, disseminação e publicação indevida de informação protegida de algum ativo de informação crítico ou de alguma atividade crítica por um período de tempo inferior ao tempo objetivo de recuperação;

XXVII - incidente cibernético: ocorrência que pode comprometer, real ou potencialmente, a disponibilidade, a integridade, a confidencialidade ou a autenticidade de sistema de informação ou das informações processadas, armazenadas ou transmitidas por esse sistema;

XXVIII - incidente de segurança: qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

XXIX - informação: dados, processados ou não, que podem ser utilizados para produção e para transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

XXX - internet: rede global, composta pela interligação de inúmeras redes;

XXXI - medidas de segurança: medidas destinadas a garantir sigilo, inviolabilidade, integridade, autenticidade e disponibilidade da informação classificada em qualquer grau de sigilo;

XXXII - plano de continuidade de negócios em segurança da informação: documentação dos procedimentos e das informações necessárias para que os órgãos ou entidades da administração pública federal mantenham seus ativos de informação críticos e a continuidade de suas atividades críticas em local alternativo, em um nível previamente definido, em caso de incidente;

XXXIII - plano de gestão de incidentes: plano de ação claramente definido e documentado, para ser usado em caso de incidente que basicamente englobe os principais recursos, serviços e outras ações que sejam necessárias para implementar o processo de gerenciamento de incidentes;

XXXIV - plano de gestão de riscos em segurança da informação: documentação que compõe o processo de gestão de riscos de segurança da informação, que deve conter, pelo menos, a abrangência da aplicação da gestão de riscos, delimitando seu âmbito de atuação e os ativos de informação que serão objeto de tratamento; a metodologia a ser utilizada que deverá contemplar, no mínimo, critérios de avaliação e de aceitação de riscos; os tipos de riscos; o nível de severidade dos riscos; um modelo do relatório de identificação, análise e avaliação dos riscos de segurança da informação com as orientações necessárias para sua elaboração; e um modelo do relatório de tratamento de riscos de segurança da informação com as

orientações necessárias para sua elaboração;

XXXV - política: intenções e diretrizes globais formalmente expressas pela direção;

XXXVI - política de segurança da informação: documento aprovado pela autoridade responsável pelo órgão ou entidade da administração pública federal, direta e indireta, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação;

XXXVII - prestador de serviço: pessoa envolvida com o desenvolvimento de atividades, de caráter temporário ou eventual, exclusivamente para o interesse do serviço, que poderão receber credencial especial de acesso;

XXXVIII - rede de computadores: conjunto de computadores, interligados por ativos de rede, capazes de trocar informações e de compartilhar recursos, por meio de um sistema de comunicação;

XXXIX - recursos de processamento da informação: qualquer sistema de processamento da informação, serviço ou infraestrutura, ou as instalações físicas que os abriguem;

XL - 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;

XLI - risco de segurança da informação: risco potencial associado à exploração de uma ou mais vulnerabilidades de um ou mais ativos de informação, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização;

XLII - segurança da informação: preservação da confidencialidade, integridade, disponibilidade, adicionalmente outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade, podem também estar envolvidas;

XLIII - serviços: meio de fornecimento de valor a clientes, com vistas a entregar os resultados que eles desejam, sem que tenham que arcar com a propriedade de determinados custos e riscos;

XLIV - SI: sigla de segurança da informação;

XLV - sistema de informação: conjunto de elementos materiais ou intelectuais, colocados à disposição dos usuários, em forma de serviços ou bens, que possibilitam a agregação dos recursos de tecnologia, informação e comunicações de forma integrada;

XLVI - tecnologia da informação: ativo estratégico que apoia processos de negócios institucionais, mediante a conjugação de recursos, processos e técnicas, utilizados para obter, processar, armazenar, disseminar e fazer uso de informações; e

XLVII - usuário: pessoa física ou jurídica, seja servidor público, estudante, prestador de serviços, fornecedor, estagiário, voluntário habilitado pela administração para acessar os ativos de informação do IFTO.

CAPÍTULO IV
DOS PRINCÍPIOS

Art. 5° As ações de segurança da informação no IFTO devem regidas pelos seguintes princípios:

I - respeito aos princípios e diretrizes constitucionais, legais e regulamentares que regem a administração pública federal;

II - garantia de integridade, autenticidade e disponibilidade da informação sob a custódia do IFTO, com respeito ao princípio da transparência e atribuição de confidencialidade apenas nos casos expressamente previstos na legislação;

III - alinhamento estratégico da Política de Segurança da Informação com os demais planos institucionais;

IV - responsabilidade pelo cumprimento das normas pertinentes à segurança da informação vigentes; e

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

CAPÍTULO V
DAS DIRETRIZES GERAIS

Art. 6° As diretrizes gerais constituem os pilares da gestão de segurança da informação no IFTO, norteando a elaboração de normas, planos, procedimentos, metodologias, ações e controles que garantem que os princípios de segurança da informação definidos nesta PSI sejam atingidos.

§ 1º O IFTO deve utilizar os guias metodológicos que serão disponibilizados pelo Gabinete de Segurança Institucional da Presidência da República em seu sítio eletrônico, para fins de implementação de ações relacionadas à gestão da segurança da informação.

§ 2º A alta administração deve apoiar ativamente a segurança da informação dentro do IFTO, por meio de um claro direcionamento, demonstrando o seu comprometimento, definindo atribuições de forma explícita e reconhecendo as responsabilidades pela segurança da informação.

§ 3º A PSI deve estar alinhada aos objetivos estratégicos, processos, requisitos legais, planos institucionais e estrutura organizacional do IFTO.

§ 4º Um plano de gestão segurança da informação deve ser definido juntamente com um orçamento adequado para a implementação das ações relacionadas à segurança da informação.

§ 5º Pessoas e sistemas devem ter o menor privilégio e o mínimo acesso aos recursos, sistemas operacionais, banco de dados, dispositivos eletrônicos, *softwares*, sistemas de informação e serviços de TI, a fim de garantir maior proteção de dados e informações.

§ 6º É expressamente proibido o uso dos meios e recursos de tecnologia da informação disponibilizados pelo IFTO para acesso, guarda ou encaminhamento de material discriminatório, malicioso, antiético ou ilegal.

§ 7º O usuário responderá pelo prejuízo que vier a ocasionar ao IFTO em decorrência do descumprimento de qualquer regra da PSI ou normas internas complementares de segurança da informação.

CAPÍTULO VI
DA GESTÃO DE SEGURANÇA DA INFORMAÇÃO

Art. 7° A gestão de segurança da informação deve ser mantida e implementada de forma contínua, buscando manter o alinhamento com a evolução da tecnologia e de seus riscos, identificando os fatores internos e externos que podem impactar no alcance dos objetivos estratégicos do IFTO.

§ 1º A gestão de segurança da informação 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 necessidades operacionais prioritárias, como também as implicações que o nível de segurança da informação pode trazer ao cumprimento dessas

exigências, conforme as diretrizes existentes na legislação pertinente.

§ 2º Os processos relacionados à gestão de segurança da informação devem estar alinhados com os controles internos de gestão do IFTO.

Seção I
Do Tratamento da Informação

Art. 8° O IFTO deve desenvolver processos, procedimentos e controles técnicos para identificar, classificar, manusear, reter e descartar dados de maneira adequada em todo o seu ciclo de vida.

§ 1º Uma política específica contendo diretrizes, competências e responsabilidades deve ser estabelecida, documentada e atualizada continuamente para proteger a troca de informações em todos os tipos de recursos de comunicação do IFTO.

§ 2º Um processo de gestão de dados deve ser estabelecido, documentado e atualizado continuamente contendo minimamente as fases de coleta, armazenamento, processamento, análise, compartilhamento, reutilização e eliminação de dados.

§ 3º Dados devem ser classificados, armazenados, processados ou acessíveis em sistemas, recursos e serviços de TI através de controles de segurança adequados.

§ 4º Procedimentos e controles para o tratamento e o armazenamento de dados devem ser estabelecidos, documentados e atualizados para proteger os dados contra a divulgação não autorizada ou uso indevido.

§ 5º O encarregado pelo tratamento de dados deve adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

§ 6º Os sistemas de informação devem ser estruturados de forma a atender aos requisitos de segurança da informação, os padrões e boas práticas de governança de dados, princípios gerais previstos na Lei Geral de Proteção de Dados e demais normas regulamentares vigentes.

§ 7º Acordos para a troca de informações entre o IFTO e entidades externas devem ser estabelecidos, documentados e atualizados continuamente de forma a manter o nível adequado de segurança da informação.

Seção II
Da Segurança Física e do Ambiente

Art. 9° A segurança física dos equipamentos e os mecanismos de proteção às instalações físicas e áreas de processamento de informações devem ser protegidas contra acesso indevido, danos e interferências em resposta aos riscos identificados pelo IFTO.

Parágrafo único. Locais onde se encontram os equipamentos de infraestrutura de TI devem ser protegidos por controles apropriados de entrada para assegurar que somente pessoas autorizadas tenham acesso.

Seção III
Da Gestão de Incidentes em Segurança da Informação

Art. 10° Os incidentes de segurança devem ser identificados, analisados, contidos, avaliados, comunicados e documentados de forma a impedir a interrupção das atividades e não afetar o

alcance dos objetivos estratégicos.

§ 1º Uma equipe de tratamento e resposta a incidentes cibernéticos deve ser estabelecida e mantida continuamente com o objetivo de evitar, na medida do possível incidentes de segurança da informação.

§ 2º Um processo de gestão de incidentes de segurança da informação deve ser estabelecido, executado, documentado e atualizado continuamente, contendo minimamente as fases identificação, análise, contenção/erradicação/recuperação e resolução, avaliação pós incidente, comunicação e documentação.

§ 3º Um plano de gestão de incidentes em segurança da informação deve ser estabelecido e mantido atualizado continuamente para identificar, analisar, conter, avaliar, comunicar e documentar incidentes relacionados à segurança da informação.

§ 4º Todos os incidentes notificados ou detectados devem ser registrados, com a finalidade de assegurar registro histórico das atividades da ETIR.

§ 5º Os membros da ETIR devem ser capacitados para operar os recursos disponíveis para a resolução de incidentes de segurança da informação.

Seção IV
Da Gestão de Ativos

Art. 11° Os ativos de informação, sistemas, banco de dados, *softwares*, aplicativos, recursos e serviços de TI devem ser protegidos contra indisponibilidade, acessos indevidos, ameaças, ataques, alterações, falhas, perdas, danos, furtos, roubos, interrupções não programadas e outros incidentes de segurança da informação.

§ 1º Regras sobre gestão de ativos devem ser estabelecidas, mantidas, documentadas e analisadas criticamente tomando-se como base os requisitos de controle de ativos e segurança da informação.

§ 2º Um processo de gestão de ativos deve ser desenvolvido em conformidade com a legislação pertinente de forma a alcançar e manter a proteção de dados adequada.

§ 3º O processo de gestão de ativos deve ser dinâmico, periódico e estruturado para manter a base de dados de ativos da informação atualizada a fim de prover informações para o desenvolvimento de ações e planos de aperfeiçoamento de práticas de gestão da segurança da informação no âmbito do IFTO.

§ 4º O processo de gestão de ativos de informação deve considerar preliminarmente: os objetivos estratégicos, processos internos, requisitos legais e estrutura organizacional do IFTO.

§ 5º O processo de gestão de ativos deve conter minimamente fases para aquisição, identificação, implementação, operação, manutenção e descarte de ativos institucionais.

§ 6º Um registro de ativos de informação deve ser mantido destinado a subsidiar os processos de gestão de riscos, de gestão de continuidade e de gestão de mudanças nos aspectos relativos à segurança da informação, bem como para os procedimentos de auditoria, conformidade e melhoria contínua.

§ 7º O registro de ativos de informação resultante do processo de mapeamento de ativos de informação deve conter: os responsáveis, proprietários e custodiantes, de cada ativo de informação; as informações básicas sobre os requisitos de segurança da informação de cada ativo de informação; os contêineres de cada ativo de informação; as interfaces de cada ativo de informação e as interdependências entre eles.

§ 8º Os ativos devem ser protegidos para reduzir os riscos de ameaças e perigos do meio ambiente, bem como as oportunidades de acesso não autorizado.

§ 9º Toda a informação que trafega pelos ativos de informação deve ser monitorada de acordo com as necessidades de segurança da informação e legislação vigente.

Seção V
Da Gestão do Uso dos Recursos Operacionais e de Comunicações

Art. 12° A gestão segura do uso dos recursos operacionais e de comunicações de tecnologia da informação envolve vários aspectos, como por exemplo: gestão de mudanças, segregação de funções, separação dos ambientes de produção, desenvolvimento e teste, gerenciamento de serviços terceirizados, planejamento e aceitação de sistemas, proteção contra códigos maliciosos e móveis, cópias de segurança, gerenciamento da segurança em redes, manuseio de mídias, troca de informações, e-mails, acesso à internet, uso seguro da nuvem computacional, acesso remoto, mídias sociais, laboratórios de informática entre outros.

§ 1º Regras para o uso seguro de recursos operacionais e de comunicação devem ser estabelecidas, mantidas, documentadas e analisadas criticamente em relação aos requisitos de privacidade e segurança da informação.

§ 2º Controles de segurança da informação devem ser implementados, mantidos e atualizados continuamente para estabelecer e manter monitoramento e defesa da rede contra ameaças de segurança em toda a infraestrutura de rede corporativa e base de usuários.

§ 3º As operações de gestão de recursos de TI deverão ser adequadamente monitoradas de forma a detectar atividades não autorizadas ou que comprometam a disponibilidade dos recursos, sistemas e serviços de TI.

§ 4º Medidas de segurança devem ser implementadas quando os usuários estão trabalhando remotamente, a fim de proteger as informações acessadas, processadas ou armazenadas fora das instalações do IFTO.

§ 5º Ferramentas e controles devem ser implementados e mantidos para impedir a instalação, disseminação e execução de aplicações, códigos ou *scripts* maliciosos em ativos institucionais.

§ 6º Dispositivos de rede devem ser gerenciados ativamente a fim de evitar que atacantes explorem serviços de rede e pontos de acesso vulneráveis.

§ 7º A aquisição, manutenção e desenvolvimento de sistemas de informação devem observar os padrões, critérios e controles de segurança da informação estabelecidos na legislação vigente.

§ 8º O ciclo de vida da segurança de *software* adquirido, desenvolvido ou hospedado deve ser gerenciado para prevenir, detectar e corrigir vulnerabilidades antes que possam afetar o IFTO.

§ 9º A implementação ou contratação de computação em nuvem deve estar em conformidade com as diretrizes desta PSI e com a legislação sobre contratação vigente na administração pública federal.

Seção VI
Dos Controles de Acesso

Art. 13° O acesso à informação disponibilizada em recursos, softwares, aplicativos, sistemas e serviços de TI deve ser gerenciado com base nos requisitos de negócio e segurança da informação adotados pelo IFTO.

§ 1º Regras para o controle de acesso devem ser estabelecidas, documentadas e analisadas criticamente tomando-se como base os requisitos de acesso seguro a recursos, sistemas, *softwares*, aplicativos e serviços de TI.

§ 2º Um processo de gestão de controle de acesso deve conter minimamente fases para identificação, autenticação e autorização de contas de usuários e serviços em sistemas operacionais, *softwares*, aplicativos, sistemas de informação, banco de dados, recursos e serviços de TI.

§ 3º Procedimentos, rotinas e ações para o controle de acesso aos ativos institucionais devem ser estabelecidos, documentados e atualizados continuamente para garantir o acesso seguro às informações, instalações e sistemas de informação.

§ 4º *Softwares* devem implementados, configurados e mantidos atualizados para atribuir e gerenciar autorização de credenciais para contas de usuário, incluindo contas de administrador, bem como contas de serviço, de ativos institucionais e *softwares*.

§ 5º A atribuição e a utilização de direitos de acesso privilegiados devem ser restringidas e geridas de forma a garantir que apenas usuários autorizados, componentes de *software* e serviços sejam fornecidos com direitos de acesso privilegiados.

Seção VII
Da Gestão de Riscos

Art. 14° O processo de gestão de riscos de segurança da informação tem por objetivo direcionar e controlar o risco de segurança da informação, a fim de adequá-lo aos níveis aceitáveis para o IFTO.

§ 1º Um processo contínuo de gestão de riscos de segurança da informação deve ser estabelecido 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 da informação, a fim de adequar riscos aos níveis aceitáveis para o IFTO.

§ 2º O processo de gestão de riscos de segurança da informação deve estar alinhado com o modelo de gestão de riscos institucional, compatível com a missão e os objetivos estratégicos do IFTO, processos internos, requisitos legais, políticas e estrutura organizacional do IFTO.

§ 3º O processo de gestão de riscos de segurança da informação deve fornecer ao IFTO os seguintes documentos: plano de gestão de riscos de segurança da informação, relatório de identificação, análise, avaliação e tratamento dos riscos de segurança da informação.

§ 4º O plano de gestão de riscos de segurança da informação deve conter, no mínimo: a abrangência da aplicação da gestão de riscos, delimitando seu âmbito de atuação e os ativos de informação que serão objeto de tratamento; a metodologia a ser utilizada que deve contemplar, no mínimo, critérios de avaliação e de aceitação de riscos; os tipos de riscos; o nível de severidade dos riscos; um modelo do relatório de identificação, análise e avaliação dos riscos de segurança da informação com as orientações necessárias para sua elaboração e um modelo do relatório de tratamento de riscos de segurança da informação com as orientações necessárias para sua elaboração; e

§ 5º O plano de gestão de riscos da segurança da informação deve ser regularmente revisado, a fim de manter atualizados os riscos relativos aos ativos de informação.

§ 6º O processo de implementação do plano de gestão de riscos de segurança da informação deve considerar, dentre outros aspectos, as recomendações de mudanças em relação aos critérios de aceitação de riscos, a abrangência da atuação do plano, as ações de segurança da informação e as atividades de tratamento de riscos previstas.

§ 7º O relatório de identificação, análise e avaliação dos riscos de segurança da informação deve ser elaborado com base no modelo estabelecido pelo plano de gestão de riscos de segurança da informação.

§ 8º O relatório de identificação, análise, avaliação e tratamento dos riscos de segurança da

informação deve ser atualizado anualmente e sempre que houver alteração em algum dos fatores de risco ou em algum contexto interno ou externo, devendo ser posteriormente enviado ao gestor de segurança da informação para aprovação.

Seção VIII
Da Gestão de Continuidade

Art. 15° A implementação do processo de gestão de continuidade de negócios envolvendo segurança da informação tem o objetivo de minimizar os impactos decorrentes de falhas, desastres ou indisponibilidades significativas sobre as atividades do IFTO, além de recuperar perdas de ativos de informação em nível aceitável, por intermédio de ações de resposta a incidentes e recuperação de desastres.

§ 1º Um processo de gestão de continuidade de negócios em segurança da informação deve ser estabelecido, documentado e atualizado continuamente com a finalidade de fornecer estrutura para assegurar a continuidade das atividades do IFTO, em caso de interrupção, assegurar a sua retomada no menor tempo possível.

§ 2º O processo de gestão de continuidade de negócios em segurança da informação deve conter minimamente as fases de planejamento e iniciação; análise de impacto nos negócios; estratégias de recuperação; desenvolvimento e implementação; e manutenção e revisão.

§ 3º O processo de gestão de continuidade de negócios em segurança da informação deve ser composto por um plano de continuidade de negócios, o qual observará o disposto no relatório de identificação, análise, avaliação e tratamento de riscos de segurança da informação e a prioridade de recuperação dos processos de negócio, considerados críticos para o IFTO.

§ 4º Um plano de continuidade de negócios em segurança da informação deve ser elaborado contendo minimamente os procedimentos e as informações necessárias para que o IFTO mantenha seus ativos de informação e a continuidade de suas atividades em local alternativo, em caso de eventos disruptivos.

§ 5º O plano de continuidade de negócios deverá ser testado regularmente, com intuito de que seus resultados sejam documentados e possam garantir a sua efetividade em caso de necessidade de ativação.

Seção IX
Da Gestão de Mudanças

Art. 16° A implementação do processo de gestão de mudanças tem por objetivo preparar e adaptar o IFTO para as mudanças decorrentes da evolução de processos e de tecnologias da informação, visando à obtenção de mudanças eficazes e eficientes e à mitigação de eventuais resistências.

§ 1º A gestão de mudanças deve preparar e adaptar o IFTO para as mudanças decorrentes da evolução de processos e de tecnologias da informação, visando à obtenção de mudanças eficientes e à mitigação de eventuais resistências.

§ 2º Um processo de gestão de mudanças deve ser estabelecido, documentado e mantido atualizado contendo minimamente fases para planejamento, implementação, monitoramento e aprendizado.

§ 3º O processo de gestão de mudanças deve ser respaldado pelas informações levantadas no relatório de identificação, análise, avaliação e tratamento de riscos de segurança da informação.

§ 4º O processo de gestão de mudanças, além de promover o controle das mudanças

planejadas, deve considerar a análise crítica das consequências de mudanças não previstas, atuando em ações para amenizar os efeitos adversos.

§ 5º Mudanças no provisionamento dos serviços, incluindo manutenção e melhoria da política de segurança da informação, dos procedimentos e controles existentes, devem ser gerenciadas levando-se em conta a criticidade dos sistemas e processos de negócio envolvidos e a reanálise/reavaliação de riscos.

§ 6º Regras para a gestão de mudanças relacionadas à segurança da informação devem ser tratadas em norma específica.

Seção X
Da Gestão de Vulnerabilidades

Art. 17° A gestão de vulnerabilidades deve ser implementada com vistas a prevenir a exploração de vulnerabilidades na infraestrutura de redes do IFTO.

§ 1º Regras para a gestão de vulnerabilidades devem ser estabelecidas, documentadas e avaliadas continuamente a fim de prevenir ataques cibernéticos.

§ 2º Um processo de gestão de vulnerabilidades deve ser estabelecido, documentado e atualizado continuamente contendo minimamente fases para identificação, avaliação, remediação e comunicação de potenciais ameaças.

§ 3º Informações sobre vulnerabilidades técnicas dos sistemas de informação em uso devem ser obtidas e a exposição do IFTO a tais vulnerabilidades deve ser avaliada, tomando medidas adequadas.

§ 4º Um programa de testes de invasão deve ser estabelecido, documentado e avaliado continuamente de forma a monitorar ameaças e vulnerabilidades, e com isso minimizar possíveis ataques cibernéticos.

§ 5º Ações de mitigação e remediação de vulnerabilidades devem ser realizadas continuamente a fim de proteger os ativos institucionais.

Seção XI
Da Gestão de Fornecedores e Terceiros

Art. 18° Os acordos com terceiros envolvendo o acesso, processamento, comunicação ou gerenciamento dos recursos, sistemas, softwares, aplicativos e serviços de TI devem cobrir todos os requisitos de segurança da informação definidos nesta política.

§ 1º Um processo para avaliar os provedores de serviços deve ser estabelecido e atualizado continuamente para proteger dados sensíveis, sistemas, *softwares*, aplicativos e serviços de TI críticos para o IFTO.

§ 2º Editais de licitação, contratos ou acordos de cooperação técnica com entidades prestadoras de serviços devem constar cláusula específica sobre a obrigatoriedade de atendimento às diretrizes de privacidade e segurança da informação adotada pelo IFTO através de suas políticas e normas internas complementares.

Seção XII
Da Gestão Registros (logs) de Auditoria

Art. 19° A gestão de registro (logs) de auditoria deve definir fases, atividades e responsabilidades para coletar, armazenar, usar, e excluir *logs* de sistemas, *softwares*,

aplicativos, bancos de dados, sistemas de informação e serviços de TI.

§ 1º Regras para registro (*logs*) de auditoria devem ser estabelecidas, documentadas e atualizadas continuamente de forma a produzir inteligência contra ameaças cibernéticas.

§ 2º Um processo de gestão de registros (*logs*) de auditoria deve ser estabelecido, executado, documentado e atualizado continuamente, contendo minimamente as fases coleta, armazenamento, uso e exclusão de eventos relacionados à recursos, redes, sistemas operacionais, *softwares*, aplicativos, sistemas de informação e serviços de TI.

§ 3º Registros (*logs*) de auditoria contendo atividades dos usuários, exceções e outros eventos de segurança da informação devem ser produzidos e mantidos por um período de tempo conforme disponibilidade de recursos tecnológicos para futuras investigações e monitoramento de controle de acesso.

§ 4º Serviços de TI disponibilizados por terceiros devem ter *logs* analisados criticamente e auditorias devem ser executadas regularmente.

§ 5º Quando possível registro de *logs* de auditoria de recursos, sistemas, *softwares*, aplicativos, banco de dados, sistemas de informação e serviços de TI devem ser mantidos, conforme recomenda a legislação pertinente.

Seção XIII
Da Auditoria e Conformidade

Art. 20° A auditoria e conformidade nos aspectos de segurança da informação deve proporcionar adequado grau de confiança a um determinado processo, mediante o atendimento de requisitos definidos em políticas, procedimentos, normas ou em regulamentos técnicos aplicáveis.

§ 1º Procedimentos apropriados de auditoria e conformidade devem ser implementados para garantir que requisitos legais e contratuais em relação a direitos de propriedade intelectual, uso de produtos e *softwares* proprietários.
§ 2º Os sistemas de informação devem ser periodicamente auditados quanto à sua conformidade com as normas de segurança da informação implementadas e legislação pertinente no âmbito da administração pública federal.

§ 3º A auditoria e conformidade deve ser realizada em recursos, sistemas, serviços, contratos, sistemas de informação, convênios, acordos de cooperação e outros instrumentos de parceria firmados pelo IFTO.

§ 4º A auditoria e conformidade poderá combinar ampla variedade de técnicas, tais como: análise de documentos, análise de registro (*logs*), análise de código-fonte, entrevistas, simulação de intrusão e testes de invasão.

§ 5º As metodologias, procedimentos e controles utilizados na auditoria e conformidade devem ser definidos em norma interna complementar conforme recomendações da legislação vigente.

Seção XIV
Da Conscientização, Educação e Treinamento em Segurança da Informação

Art. 21° Esta PSI e suas atualizações, bem como políticas e normas internas complementares de segurança da informação do IFTO devem ser divulgadas amplamente a todos os usuários, a fim de promover sua observância, seu conhecimento, bem como a formação da cultura de segurança da informação.

Parágrafo único. Um programa de conscientização, educação e treinamento em segurança da informação deve ser estabelecido, documentado e atualizado continuamente para influenciar o

comportamento dos usuários em relação a atitudes seguras em relação às ameaças cibernéticas.

CAPÍTULO VII
DAS COMPETÊNCIAS, ATRIBUIÇÕES E RESPONSABILIDADES

Art. 22° A segurança da informação é dever de todos os usuários que utilizam os recursos, sistemas, *softwares*, aplicativos, sistemas de informação e serviços de TI. Para isso os usuários devem ter hábitos, posturas e cuidados em relação à proteção e privacidade de dados.

Seção I

Da Alta Administração

Art. 23° Compete à alta administração as seguintes responsabilidades:

I - prover a orientação e o apoio necessário às ações de segurança da informação, de acordo com os objetivos estratégicos, planos institucionais, estrutura organizacional, leis e regulamentos pertinentes;

II - garantir os recursos (humanos, tecnológicos e financeiros) necessários para a execução de ações relacionadas a execução da Política de Segurança da Informação no âmbito do IFTO;

III - aprovar os processos de segurança da informação;

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

V - coordenar e executar as ações de segurança da informação no âmbito de sua atuação;

VI - designar ao menos um servidor efetivo lotado no IFTO, como responsável pela avaliação de conformidade de acordo com os aspectos relativos à segurança da informação;

VII - consolidar e analisar os resultado dos trabalhos de auditoria sobre gestão de segurança da informação; e

VIII - aplicar as ações corretivas e administrativas cabíveis, nos casos de violação da segurança da informação.

Seção II

Do Gestor de Tecnologia da Informação

Art. 24° Compete ao Gestor de Tecnologia da Informação as seguintes responsabilidades:

I - planejar, implementar e melhorar continuamente os controles de privacidade e segurança da informação em soluções de tecnologia da informação e comunicações, nos termos da legislação vigente na administração pública federal.

Seção III

Do Gestor de Segurança da Informação

Art. 25° Compete ao Gestor de Segurança da Informação as seguintes responsabilidades:

I - coordenar o Comitê de Segurança da Informação;

II - coordenar a elaboração da Política de Segurança da Informação e das normas internas complementares de segurança da informação do IFTO, observadas as recomendações exaradas pelo Gabinete de Segurança Institucional da Presidência da República;

III - assessorar a alta administração na implementação da Política de Segurança da Informação;

IV - coordenar o processo de mapeamento de ativos de informação, bem como designar um agente responsável pela gestão dos ativos de informação, dentre os servidores efetivos do IFTO;

V - coordenar a gestão de riscos de segurança da informação, bem como designar o agente responsável pela gestão de riscos de segurança da informação, dentre os servidores efetivos do IFTO;

VI - aprovar o plano de gestão de riscos de segurança da informação e os relatórios de identificação, análise, avaliação e tratamento de riscos;

VII - coordenar o processo de gestão de continuidade de negócios em segurança da informação, bem como designar um agente responsável pela referida gestão, dentre os servidores efetivos do IFTO;

VIII - coordenar a gestão de mudanças no que se refere à segurança da informação, bem como designar o o agente responsável pela gestão de mudança relacionada a segurança da informação, dentre os servidores efetivos do IFTO;

IX - proporcionar a interação constante entre as equipes de gestão de mudanças em aspectos de segurança da informação, de gestão de riscos de segurança da informação e de gestão de continuidade de negócios em segurança da informação;

X - fornecer, ao(s) agente(s) responsável(is) pela avaliação de conformidade, todas as informações necessárias ao processo de gestão de conformidade nos aspectos de segurança da informação;

XI - emitir parecer técnico sobre o relatório de avaliação de conformidade e apresentá-los ao Comitê de Segurança da Informação;

XII - adotar as medidas necessárias para atender às recomendações do relatório de avaliação de conformidade aprovado pela alta administração;

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

XIV - promover, com apoio da alta administração, a ampla divulgação da PSI, das normas internas complementares de segurança da informação e de suas atualizações, de forma ampla e acessível, a todos os usuários, a fim de que esses tomem conhecimento de tais instrumentos;

XV - incentivar estudos de novas tecnologias, bem como seus eventuais impactos relacionados à segurança da informação;

XVI - propor recursos e medidas necessárias a execução de ações de segurança da informação;

XVII - acompanhar os trabalhos da Equipe de Tratamento e Resposta a Incidentes Cibernéticos;

XVIII - verificar os resultados dos trabalhos de auditoria sobre a gestão da segurança da informação;

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

XX - coordenar ações de gestão de segurança da informação em âmbito institucional;

XXI - fomentar e coordenar ações periódicas de conscientização e de treinamento em segurança da informação para todas as partes interessadas, incluindo autoridades, servidores e colaboradores; e

XXII - manter contato direto com o Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República em assuntos relativos à segurança da informação.

Seção IV

Do Comitê de Segurança da Informação

Art. 26° Compete ao Comitê de Segurança da Informação as seguintes responsabilidades:

I - assessorar a implementação das ações de segurança da informação;

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 complementares de segurança da informação;

IV - propor alterações à Política de Segurança da Informação e às normas internas complementares de segurança da informação; e

V - deliberar sobre normas internas complementares de segurança da informação.

Seção V

Da Equipe de Tratamento e Resposta a Incidentes Cibernéticos

Art. 27° Compete à Equipe de Tratamento e Resposta a Incidentes Cibernéticos:

I - atuar conforme normativos, padrões e procedimentos técnicos exarados pelo Centro de Tratamento e Resposta de Incidentes Cibernéticos do governo federal, sem prejuízo das demais metodologias e padrões conhecidos.

Seção VI

Da Unidade de Controle Interno

Art. 28° Compete à Unidade de Controle Interno a seguinte responsabilidade:

I - atuar no apoio, supervisão e monitoramento das atividades desenvolvidas pela primeira linha de defesa de segurança da informação conforme legislação pertinente.

Seção VII

Da Diretoria de Tecnologia da Informação e demais setores de TI das unidades do IFTO

Art. 29° Compete à Diretoria de Tecnologia da Informação e demais setores de TI das unidades do IFTO as seguintes responsabilidades:

I - pesquisar, implantar e manter soluções de segurança da informação no âmbito do IFTO;

II - gerenciar os ativos de informação;

III - gerenciar o controle de acesso à rede de comunicação de dados e aos sistemas informatizados do IFTO;

IV - realizar a gestão de riscos de segurança da informação;

V - elaborar o plano de gestão de riscos de segurança da informação;

VI - elaborar o relatório de identificação, análise e avaliação dos riscos;

VII - elaborar o relatório de tratamento de riscos de segurança da informação;

VIII - propor as diretrizes a serem contempladas no plano de continuidade de negócios em segurança da informação;

IX - propor ações para o plano de continuidade de negócios em segurança da informação;

X - realizar os testes de funcionamento do plano de continuidade de negócios em segurança da informação;

XI - avaliar e aprimorar o plano de continuidade de negócios a partir dos resultados dos testes de funcionamento;

XII - gerenciar a contingência quando ocorrer a interrupção de atividades, com base nesse plano desenvolvido;

XIII - propor os recursos necessários para a implementação e o desenvolvimento das ações relacionadas à continuidade das atividades, bem como para a realização dos testes de funcionamento do plano de continuidade de negócios;

XIV - propor melhorias na implementação de novos controles relativos ao plano de continuidade de negócios em segurança da informação;

XV - participar da elaboração da análise de impacto nos negócios;

XVI - propor medidas visando ao desenvolvimento da cultura de gestão de continuidade de negócios em segurança da informação;

XVII - recomendar à alta administração a instituição de um grupo técnico de mudança, composto por servidores das áreas afetadas e da área de segurança da informação para a elaboração do documento de avaliação e aprovação de mudança;

XVIII - elaborar, juntamente com o grupo técnico de mudança, o documento de avaliação e aprovação de mudança e submetê-lo à análise do gestor de segurança da informação;

XIX - acompanhar, juntamente com o grupo técnico de mudança, os testes da mudança aprovada pelo documento de avaliação e aprovação de mudança;
XX - acompanhar, juntamente com o grupo técnico de mudança, a implementação da solução aprovada no documento de avaliação e aprovação de mudança;
XXI - assegurar, juntamente com o grupo técnico de mudança, registro de auditoria contendo todas as informações relevantes relacionadas com a mudança;

XXII - informar ao gestor de segurança da informação sobre o andamento e a conclusão do processo;

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

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

XXV - propor e gerenciar procedimentos de segurança da informação para a rede de comunicação de dados do IFTO;

XXVI - implantar, gerenciar e monitorar a estrutura de ativos institucionais no âmbito do IFTO;

XXVII - administrar a rede corporativa do IFTO, garantindo o acesso e a segurança das

informações;

XXVIII - pesquisar e manter atualizada a definição de normas, padrões e mecanismos de administração da rede de computadores, visando à segurança e o desempenho dos serviços de Tecnologia da Informação no IFTO; e

XXIX - instalar, configurar e manter atualizados controles de segurança da informação.

Seção VIII

Dos Gestores da Informação

Art. 30° Compete aos gestores da informação as seguintes responsabilidades:

I - adotar as medidas e procedimentos necessários para garantir a segurança das informações;
II - definir procedimentos, critérios de acesso e classificar as informações, observados os dispositivos legais e regimentais relativos ao sigilo e a outros requisitos de classificação pertinentes, considerando os procedimentos da Lei de Acesso à Informação – LAI, e o Serviço de Informação ao Cidadão – SIC, no âmbito da IFTO;
III - propor regras específicas ao uso das informações;
IV - manter o devido registro e controle ao autorizar e fornecer acesso aos ativos de TI sob sua responsabilidade aos usuários; e
V - observar as diretrizes da Lei Geral de Proteção de Dados Pessoais – LGPD.

Seção IX

Do Custodiante da Informação

Art. 31° Compete ao Custodiante da Informação as seguintes responsabilidades:

I - garantir a segurança da informação e proteção dos dados sob sua custódia;
II - comunicar oportunamente a ETIR sobre situações que comprometam a segurança das informações e a proteção dos dados sob sua custódia;
III - comunicar a ETIR eventuais limitações para cumprimento dos critérios definidos para segurança da informação e proteção dos dados;
IV - observar procedimentos, critérios de acesso e classificação das informações definidos pelos gestores da informação;

V - cumprir e zelar pela observância integral das diretrizes da PSI e demais normas internas complementares e procedimentos decorrente;

VI - zelar pela disponibilidade, integridade, e autenticidade das informações e recursos em qualquer suporte sob sua custódia, bem como sua confidencialidade, quando cabível;

VII - proteger as informações contra acesso, modificação, destruição ou divulgação não autorizados; e

VIII - adotar medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os ativos de informação sob sua custódia.

Seção X

Do Proprietário da Informação

Art. 32° Compete ao proprietário da informação a seguinte responsabilidade:

I - definir o valor do ativo de informação e quais tipos de controles de segurança devem serm implementados para proteger as informações;

II - autorizar o acesso a informação;

III - proteger a informação; e

IV - comunicar ao setor de TI acerca do ingresso, alteração de lotação ou localização, e do desligamento de servidor, estagiário, voluntário, prestador de serviço ou colaborador em sua unidade organizacional.

Seção XI

Do Encarregado pelo Tratamento de Dados

Art. 33° Compete ao Encarregado de Tratamento de Dados as seguintes responsabilidades:

I - conduzir o diagnóstico de privacidade de dados; e

II - orientar, no que couber, os gestores proprietários dos ativos de informação, responsáveis pelo planejamento, implementação e melhoria contínua dos controles de privacidade em ativos de informação que realizem o tratamento de dados pessoais ou dados pessoais sensíveis, a respeito das práticas a serem tomadas em relação à proteção de dados pessoais, nos termos da legislação vigente no âmbito da administração pública federal.

Seção XII

Da Direção Geral das Unidades e Responsáveis por Setores

Art. 34° Compete aos Diretores Gerais das Unidades e responsáveis por setores as seguintes responsabilidades:

I - garantir que as atividades desempenhadas sob sua gestão estejam de acordo com a PSI;

II - incentivar a capacitação dos recursos humanos sob sua gestão em temas relacionados à segurança da informação;

III - acompanhar a execução das ações de segurança da informação no seu âmbito de atuação;

IV - estimular a cultura de segurança da informação e gestão de continuidade de negócios;

V - disseminar normas, regras, procedimentos, medidas, controles e boas práticas de segurança da informação;

VI - conscientizar os usuários de sua unidade ou setor em relação aos conceitos e às praticas de segurança da informação;

VII - incorporar aos processos de trabalho de sua unidade ou setor, práticas inerentes à segurança da informação; e

VIII - tomar as medidas administrativas necessárias para que sejam aplicadas ações corretivas nos casos de comprometimento da segurança da informação por parte dos usuários sob sua supervisão.

Seção XIII

Dos Usuários

Art. 35° Compete aos usuários as seguintes responsabilidades:

I - atender aos princípios e diretrizes contidos nesta PSI, incluindo normas e procedimentos complementares destinados à segurança da informação e comunicação;

II - guiar-se pelos princípios de confidencialidade, autenticidade, integridade, não repúdio, conformidade, controle de acesso e disponibilidade no decorrer de suas atividades;

III - zelar pelo sigilo e integridade das informações e dos ativos institucionais aos quais tiver acesso;

IV - adotar boas práticas de proteção de dados e segurança da informação;

V - responder por seus atos e acessos que causem danos ou prejuízos às informações e aos ativos no âmbito do IFTO, ou violem as regras dispostas na PSI ou em seus instrumentos complementares;

VI - respeitar a legislação e as normas de propriedade intelectual, proteção de dados e privacidade de informações pessoais pertinentes;
VII - comunicar ao IFTO sempre que tomar ciência de evento adverso que possa configurar incidente de segurança da informação;

VIII - observar restrições em relação à instalação e manutenção de *software* e *hardware*;

IX - colaborar com as investigações de incidentes de segurança da informação;

X - não usar a identificação de acesso e senha de terceiros;

XI - manter sigilo e trocar periodicamente a senha pessoal de acesso aos recursos, sistemas operacionais, *softwares*, aplicativos, sistemas de informação e serviços de TI;

XII - preservar o conteúdo das informações sigilosas a que tiver acesso, à informação cujo grau de sigilo não seja compatível com a sua credencial de segurança ou cujo teor não tenha autorização ou necessidade de conhecer;

XIII - não utilizar o ambiente computacional do IFTO para acessar, transmitir, copiar ou reter conteúdo ou arquivos com textos, fotos, filmes ou quaisquer outros registros que estejam em desacordo com a legislação vigente.

XIV - realizar *backup* de dados pessoais armazenados em ativos de TI periodicamente ou quando houver necessidade de formatação do sistema operacional, das informações contidas em computadores sob sua responsabilidade; e

XV - devolver todos os ativos institucionais em sua posse após a mudança ou encerramento da contratação ou acordo.

CAPÍTULO VIII
DAS PENALIDADES

Art. 36° Ações que violem esta PSI, diretrizes, políticas e normas internas complementares, procedimentos, ou que quebrem os controles de segurança da informação serão passíveis de investigação, podendo implicar em penas e sanções legais impostas por meio de medidas administrativas, sem prejuízo das demais medidas cíveis e penais cabíveis.

§ 1º É vedada qualquer ação que não esteja explicitamente permitida na Política de Segurança do IFTO ou que não tenha sido previamente autorizada pelo Comitê de Segurança da Informação.

§ 2º Casos omissos não tratados nesta PSI serão submetidos, analisados, tratados e decididos pelo Comitê de Segurança da Informação.

CAPÍTULO IX
DA POLÍTICA DE ATUALIZAÇÃO

Art. 37° Esta PSI bem como as políticas e normas internas complementares geradas a partir dela deverão ser revisadas, aprovadas e atualizadas em função de alterações nas normativas do IFTO, legislação pertinente, diretrizes e políticas do governo federal ou quando considerada necessária pelo Comitê de Segurança da Informação, não devendo exceder 4 (quatro) anos.

CAPÍTULO X
DAS DISPOSIÇÕES FINAIS

Art. 38° Esta PSI e suas atualizações, bem como políticas e normas internas complementares específicas de segurança da informação do IFTO, devem ser divulgadas amplamente a todos os usuários, a fim de promover sua observância, seu conhecimento, bem como a formação da cultura de segurança da informação.

Art. 39° A alta administração deve disponibilizar os recursos (humanos, tecnológicos e financeiros) necessários para a execução das diretrizes contidas nesta política.

Art. 40° Esta política entra em vigor a partir da data de sua publicação.

Documento assinado eletronicamente por **Fabiana Ferreira Cardoso**, **Gestora de Segurança da Informação**, em 19/12/2023, às 10:34, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Kleyton Matos Moreira**, **Diretor**, em 22/12/2023, às 16:19, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site http://sei.ifto.edu.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **2222382** e o código CRC **652CE69A**.

Avenida Joaquim Teotônio Segurado
Quadra 202 Sul, ACSU-SE 20, Conjunto 1, Lote 8 - Plano Diretor Sul
CEP 77020-450 Palmas - TO
(63) 3229-2200
www.ifto.edu.br - reitoria@ifto.edu.br

Referência: Processo nº 23235.010071/2020-14 SEI nº 2222382