Ministério da Educação
Secretaria de Educação Profissional e Tecnológica
Instituto Federal de Educação, Ciência e Tecnologia do Tocantins
Conselho Superior

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Aprovada pela Resolução nº 29/2020/CONSUP/IFTO, de 13 de agosto de 2020.

Dispõe sobre a Política de Segurança da Informação no âmbito do Instituto Federal de Educação, Ciência e Tecnologia do Tocantins.

CAPÍTULO I
DO OBJETIVO

Art. 1º A Política de Segurança da Informação (PSI) é uma declaração formal do Instituto Federal de Educação, Ciência e Tecnologia do Tocantins (IFTO) acerca do seu compromisso 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 IFTO.

Art. 2º A Política de Segurança da Informação tem por objetivo a instituição de diretrizes estratégicas que visam garantir disponibilidade, integridade, confidencialidade e autenticidade das informações, bem como atitudes adequadas para manuseio, tratamento, controle e proteção dos dados, informações, documentos e conhecimentos produzidos, armazenados, sob guarda ou transmitidos por qualquer meio ou recurso do IFTO contra ameaças e vulnerabilidades relacionadas à segurança da informação. Desse modo, a PSI busca preservar os ativos de informação pertencentes ao IFTO, 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 IFTO. A PSI norteia o IFTO quanto à garantia dos princípios de segurança da informação: disponibilidade, integridade, confidencialidade e autenticidade.

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 IFTO.

CAPÍTULO III
DA CONCEITUAÇÃO

Art. 5º Para fins de uniformidade dos procedimentos contidos nesta PSI, 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 IFTO.

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

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 - Comitê de Segurança da Informação (CSI): grupo de pessoas com a responsabilidade de assessorar a implementação das ações de segurança da informação e comunicações no âmbito do IFTO.

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 - Plano de Continuidade do Negócio: descreve as ações que o IFTO deve tomar para assegurar a continuidade dos processos críticos em caso de sinistros na instituição ou falhas nos sistemas, incluindo a ativação de processos manuais, duplicidade de recursos, traslado de pessoal e acionamento de prestadores de serviço.

XIII - Política de Segurança da Informação: recomendações com o propósito de estabelecer critérios para o adequado manuseio, armazenamento, transporte e descarte das informações através do desenvolvimento de diretrizes, normas, procedimentos e instruções destinadas, respectivamente, aos níveis estratégico, tático e operacional.

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

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

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

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

XVIII - 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 IFTO, de acordo com o estabelecido em normas específicas.

XIX - 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 IFTO atua em conformidade com os procedimentos estabelecidos nesta PSI, 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.

CAPÍTULO V
DOS REQUISITOS

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 - 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.

IV - 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.

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

VI - 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).

VII - 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.

VIII - 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.

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

X - 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.

XI - 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.

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

XIII - 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.

XIV - 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.

XV - 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.

XVI - 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 a pratiquem dentro do IFTO. São elas:

I - O IFTO deve instituir uma estrutura organizacional estratégica de Gestão de Segurança da Informação (GSI), refletida no seu Regimento Interno, com a responsabilidade de executar os processos de Segurança da Informação.

II - A Gestão de SI do IFTO 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 IFTO 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 IFTO 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 IFTO 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 IFTO 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 direção, em conformidade com normas complementares, manuais de procedimentos e legislação específica de SI, buscando a certificação do atendimento dos requisitos de segurança da informação. A alta direção poderá se valer de grupos internos ou externos para consecução de auditorias.

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 IFTO. 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
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): aprova a Política de Segurança da Informação e suas revisões, designa os proprietários da informação se necessário, e toma as 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): 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; pelo acompanhamento e alocação de recursos humanos e tecnológicos, projetos e iniciativas de Segurança da Informação; pela definição sobre a existência de área específica para Gestão da Segurança da Informação voltada para Gestão de Riscos; 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, trilhas de auditoria, 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 - Diretoria de Gestão de Pessoas (DGP): executa as ações de treinamento e desenvolvimento referentes à Segurança da Informação, bem como colhe a assinatura do Termo de Responsabilidade dos servidores, colaboradores, estagiários, terceirizados e voluntários. 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 - Diretoria de Comunicação (DICOM): executa as atividades relacionadas à comunicação institucional, divulgando e disseminando as orientações emanadas pela Política de Segurança da Informação.

VI - Equipe de Segurança da Informação: desenvolve, implementa e monitora estratégias de segurança que atendam aos objetivos estratégicos do IFTO; avalia, seleciona, utiliza, administra e monitora controles apropriados de proteção dos ativos de informação; conscientiza os usuários a respeito da implementação desses controles e verifica se todos os usuários colaboram com as medidas de segurança implantadas.

VII - Gestores Administrativos: multiplica e catalisa os princípios de segurança; autoriza concessão, transferência e revogação de acessos; responde conjuntamente pelas ações realizadas por seus subordinados; conscientiza os usuários sob sua supervisão em relação aos conceitos e às práticas de SI; incorpora aos processos de trabalho de sua unidade, ou de sua área, práticas inerentes à SI; toma as medidas administrativas necessárias para que sejam aplicadas ações corretivas nos casos de comprometimento da SI por parte dos usuários sob sua supervisão.

VIII - Proprietário da Informação: responsável por proteger e manter as informações e controlar o acesso conforme requisitos definidos pelo gestor da informação e em conformidade com esta PSI. Trata e classifica a informação, define os requisitos de segurança para os ativos sob sua responsabilidade, concede e revoga acessos e autoriza a divulgação de informações.

IX - Usuários: observa e acata 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, contata a DTI para tomada ações cabíveis; protege os ativos de informação do IFTO, incluindo informação, evitando perda ou modificação de dados, **software** e **hardware**; observa restrições em relação a cópias e divulgação de informações, e uso dos acordos de confidencialidade; observa restrições em relação à manutenção e instalação de **software** e **hardware**; atende à política de controle de acesso do IFTO; relata incidentes de segurança da informação e violação da segurança; atende aos princípios e diretrizes contidos nesta PSI, incluindo normas e procedimentos complementares destinados à SI; é responsável por todos os atos praticados com suas identificações (**login**, crachá, carimbo, **e-mail**, assinatura digital, etc.).

CAPÍTULO VIII
DA CAPACITAÇÃO E APERFEIÇOAMENTO

Art. 10. Os usuários devem ser continuamente capacitados para o uso dos ativos de informação quando da realização de suas atividades.

Art. 11. Programas de conscientização sobre segurança da informação serão implementados através de treinamentos específicos, assegurando que todos os colaboradores sejam informados sobre os potenciais riscos de segurança e o tipo de exposição a que estão submetidos os sistemas de informações e operações do IFTO e suas partes interessadas.

Art. 12. Os treinamentos a serem disponibilizados devem estar compatíveis com as tecnologias atualmente implementadas no ambiente informatizado, e pelas demais que porventura venham a ser adotadas.

CAPÍTULO IX
DO ACESSO, PROTEÇÃO E GUARDA DA INFORMAÇÃO

Art. 13. O acesso à informação dentro da rede do IFTO deve ser realizado através de credenciais de acesso obtidos por meio zde abertura de chamado na central de serviços no Sistema Unificado de Administração Pública (SUAP).

Art. 14. A informação deve ser protegida de acordo com o seu valor, sensibilidade e criticidade.

Art. 15. Toda e qualquer informação gerada, adquirida, utilizada ou armazenada pelo IFTO 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. 16. Todos os usuários que manipulem ou tenham acesso a informações identificadas como reservadas sob custódia ou propriedade do IFTO 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 IFTO sem autorização formal.

Art. 17. 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. 18. Os recursos computacionais disponibilizados pelo IFTO são fornecidos com o propósito único de garantir o bom desempenho das atividades do IFTO, 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 IFTO.

Art. 19. Os acessos à rede de dados do IFTO 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. 20. Todos os ativos de informação do parque computacional devem ser inventariados, incluindo-se dispositivos móveis como **notebooks**, **handsets**, **tablets** e **smartphones**, quando pertencentes ao IFTO, 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 XI
DA COMUNICAÇÃO ELETRÔNICA

Art. 21. Toda informação veiculada eletronicamente será alvo de controle e monitoração, e seu uso deve ser tão somente para fins educacionais e administrativos, sem posicionamento pessoal, político, sexual ou religioso, devendo seu comportamento ser decoroso e de acordo com a legislação em redes sociais e assemelhados, quando se identificar como usuário do IFTO, mantendo as informações de caráter reservado protegidas e comunicando ao CSI quaisquer eventos de quebra de segurança, tais como recebimento de informação sigilosa por engano, ataques, adulteração e roubo de informação.

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

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

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

CAPÍTULO XIII
DO PLANO DE CONTINUIDADE DE NEGÓCIO

Art. 23. 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 XIV
DA CONFORMIDADE

Art. 24. 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. 25. Os processos de aquisição de bens e serviços, especialmente dos ativos de informação, devem estar em conformidade com esta PSI.

Art. 26. 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 XV
DA CLASSIFICAÇÃO E DO SIGILO DA INFORMAÇÃO

Art. 27. Será passível de classificação qualquer informação que provoque riscos à vida, segurança ou saúde da população, ou riscos à defesa, economia ou relações internacionais do Estado, e aquela que, no âmbito do IFTO, provoque assimetria competitiva ou privilégio entre agentes regulados, exponha o IFTO a ataques ou fraudes, ou que pertença a normas, autorizações, estudos e fiscalizações que componham processo não concluído.

Art. 28. Informação classificada com disponibilidade crítica, se houver, deverá estar coberta pelo Plano de Continuidade do Negócio.

Art. 29. Toda informação classificada será considerada de integridade controlada.

Parágrafo único. A Política de Segurança da Informação e os Sistemas de Informação do IFTO deverão garantir a executoriedade do sigilo resultante da classificação da informação, a ser regulamentada em norma específica, e também a disponibilidade, integridade, autenticidade e confidencialidade da Informação do IFTO, independentemente de sua classificação.

CAPÍTULO XVI
DA AVALIAÇÃO E DA REGULAMENTAÇÃO

Art. 30. O cumprimento desta PSI deve ser avaliado periodicamente, de acordo com os critérios do CSI.

Art. 31. Fica a DTI autorizada a regulamentar e submeter à Reitoria do IFTO, 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 IFTO.

CAPÍTULO XVII
DAS PENALIDADES

Art. 32. O descumprimento ou violação da Política de Segurança da Informação poderá resultar na aplicação das sanções administrativas e/ou legais previstas na legislação vigente, conforme avaliação e orientação do CSI.

Art. 33. Os casos omissos serão analisados e deliberados pelo CSI do IFTO.

Art. 34. É vedada qualquer ação que não esteja explicitamente permitida na Política de Segurança do IFTO ou que não tenha sido previamente autorizada pelo CSI.

CAPÍTULO XVIII
DAS DISPOSIÇÕES FINAIS

Art. 35. A Política de Segurança da Informação será revisada e atualizada anualmente, ou sempre que ocorrerem eventos ou fatores relevantes que exijam sua revisão imediata.

Palmas, 13 de agosto de 2020.

PAULA KARINI DIAS FERREIRA AMORIM

PAULA KARINI DIAS FERREIRA AMORIM
Presidente do Comitê Gestor de Tecnologia da Informação
Portaria nº 242/2019/REI/IFTO, de 28 de fevereiro de 2019

ANTONIO DA LUZ JÚNIOR
Presidente do Conselho Superior do Instituto Federal do Tocantins

Documento assinado eletronicamente por **Paula Karini Dias Ferreira Amorim**, **Presidente**, em 18/09/2020, às 18:15, 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 **Antonio da Luz Júnior**, **Presidente**, em 21/09/2020, às 13:49, 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 **1058383** e o código CRC **5212A061**.

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
portal.ifto.edu.br — reitoria@ifto.edu.br

Referência: Processo nº 23235.010071/2020-14 SEI nº 1058383