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

POLÍTICA DE GESTÃO DO CONTROLE DE ACESSO

Estabelece a Política de Gestão do Controle de Acesso no âmbito do Instituto Federal de Educação, Ciência e Tecnologia do Tocantins (IFTO).

CAPÍTULO I
DO ESCOPO

Art. 1º A Política de Gestão do Controle de Acesso tem como objetivo estabelecer diretrizes, competências e responsabilidades para sistematizar controles de identificação, autenticação e autorização para salvaguardar as informações do IFTO, estejam elas em qualquer meio, seja físico ou digital, a fim de evitar a quebra de segurança da informação e quaisquer acessos não autorizados que implique em risco de destruição, alteração, perda, roubo ou divulgação indevida.

Art. 2º Esta política abrange diretrizes, competências e responsabilidades sobre como o acesso às informações e recursos são concedidos, monitorados e revogados dentro do IFTO de forma a garantir que apenas pessoas autorizadas tenham acesso às informações e recursos necessários para desempenhar suas funções, minimizando assim o risco de violações de segurança e vazamento de dados. Ela inclui diversos elementos, como por exemplo:

I - identificação e autenticação de usuários;

II - determina quais recursos, sistemas ou informações os usuários tem permissão para acessar após a autenticação bem sucedida (definição de privilégios e níveis de acesso de acordo com as responsabilidades de cada usuário);

III - gerencia o acesso a sistemas, dados digitais, acesso físico a edifícios, salas de servidor e outros locais que abrigam informações críticas;

IV - estabelece práticas para monitorar e registrar as atividades de acesso para identificar potenciais ameaças ou violações de segurança;

V - define diretrizes para revogar o acesso de um usuário, como por exemplo demissão, mudança de função ou quando o acesso se torna desnecessário para suas responsabilidades;

VI - envolve a conscientização de usuários sobre a importância do controle de acesso, as melhores práticas de segurança e a importância de proteger as credenciais de acesso.

CAPÍTULO II
DOS CONCEITOS E DEFINIÇÕES

Art. 3º Para fins de compreensão dos termos utilizados nesta política serão utilizados os seguintes conceitos e definições:

I - acesso: ato de ingressar, transitar, conhecer ou consultar a informação, bem como possibilidade de usar os ativos de informação de um órgão ou entidade, observada eventual restrição que se aplique;

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

III - 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;

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

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

VI - 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;

VII - *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;

VIII - 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;

IX - 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;

X - 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;

XI - conta de serviço: conta de acesso à rede corporativa de computadores, necessária a um procedimento automático (aplicação, *script*, entre outros) sem qualquer intervenção humana no seu uso;

XII - 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;

XIII - 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;

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

XV - 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;

XVI - 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;

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

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

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

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

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

XXII - 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;

XXIII - 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;

XXIV - 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;

XXV - *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;

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 - mfa: sigla de autenticação de multifatores (*multifactor authentication*);

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

XXXIV - 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;

XXXV - 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;

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

XXXVII - 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;

XXXVIII - 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;

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

XL - 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;

XLI - SI: sigla de segurança da informação;

XLII - 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;

XLIII - 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

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

CAPÍTULO III
DOS PRINCÍPIOS

Art. 4º Esta política considera os 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 IV

DAS DIRETRIZES GERAIS

Art. 5º As diretrizes gerais constituem os pilares do controle de acesso no IFTO, orientando a elaboração de norma, processo, planos, procedimentos, metodologia e ações de controle que garantem que os princípios básicos de segurança da informação sejam alcançados.

§ 1º Um procedimento operacional padrão deve ser estabelecido, documentado e atualizado para implementar controles de acesso físicos e lógicos à informação e aos ativos associados à informação que são por ele gerenciados ou custodiados, com objetivo de proteger adequadamente a confidencialidade das informações não públicas, bem como a integridade e a disponibilidade das informações consideradas críticas para o negócio.

§ 2º os controles de acesso devem ser implementados para identificação, autenticação e autorização garantindo que apenas usuários autorizados tenham acesso físico ou lógico aos recursos, sistemas ou serviços de TI.

§ 3º Rotinas devem ser configuradas para criar, atribuir, gerenciar e revogar credenciais de acesso e privilégios para contas de usuário, administrador e serviço para ativos e *software* institucionais devem ser estabelecidas e mantidas atualizadas.

§ 4º Sempre que possível controles de acesso devem ser implementados conforme necessidade legítima que justifique o acesso à informação por pessoa, sistema ou entidade, seguindo o princípio "privilégio mínimo", o qual estabelece que o perfil de acesso concedido deve incluir apenas os poderes necessários para atender as legítimas necessidades.

§ 5º Quando possível, os controles de acesso lógicos no IFTO devem utilizar autenticação com certificado digital, a fim de proporcionar uma identificação inequívoca de pessoas físicas e jurídicas, assim como comprovação de autoria em transações digitais.

§ 6º Os direitos de acesso lógicos e físicos devem ser analisados criticamente, a intervalos regulares, para remover direitos que deixaram de ser necessários e para assegurar que privilégios indevidos não foram obtidos.

§ 7º Os controles de autorização, identificação e autenticação devem garantir que apenas usuários autorizados tenham acesso físico ou façam uso dos sistemas de informação do IFTO.

CAPÍTULO V
DA GESTÃO DO CONTROLE DE ACESSO

Art. 6º O processo de gestão do controle de acesso deve estabelecer critérios para identificação, autenticação e autorização de forma a salvaguardar as informações do IFTO, estejam elas em qualquer meio, seja digital ou físico, a fim de evitar a quebra da segurança da informação e quaisquer acessos não autorizados que impliquem em risco de destruição, alteração, perda, roubo ou divulgação indevida.

Seção I
Identificação

Art. 7º A identificação de usuários deve garantir que apenas usuários autorizados obtenham acessos aos recursos, sistemas, *softwares,* sistemas de informação e serviços de TI.

§ 1º Os usuários terão direito de acesso lógico aos recursos da rede local, sistemas, *softwares*, sistemas de informação e serviços de TI, quando devidamente identificados através de recursos, serviços ou sistemas informatizados do IFTO.

§ 2º Um inventário centralizado de todas as contas de usuários e serviços deve ser estabelecido, documentado e mantido atualizado continuamente por meio de serviço de diretório ou de identidade.

§ 3º Um procedimento padronizado para o registro de usuários deve ser estabelecido, documentado e atualizado continuamente.

§ 4º Um procedimento padronizado para a suspensão e exclusão de usuários deve ser estabelecido, documentado e atualizado continuamente.

§ 5º Os usuários deverão ser identificados por meio de credenciais como nome de usuário e senha, autenticação biométrica, cartões de acesso etc.

§ 6º Ao criar as credenciais de acesso o sistema deve definir uma senha temporária que deve ser alterada no primeiro acesso à rede IFTO.

§ 7º Sempre que possível as senhas dos usuários devem ser únicas.

§ 8º Um usuário ao ser criado deve ter o mínimo de privilégios existentes nos ativos, recursos e serviços de TI.

§ 9º As informações de credenciais devem ser armazenadas de forma segura.

§ 10º Em caso de perda de senha de acesso aos ativos, recursos e serviços de TI o usuário deve acessar sistema de informação SUAP e realizar o procedimento de recuperação de senha indicado.

§ 11º Caso o usuário não consiga realizar o procedimento de recuperação de senhas, ele deve procurar o setor de gestão de pessoas, caso seja servidor, fornecedor ou prestador de serviços; setor de registro escolar, caso seja estudante; e demais usuários, o setor de TI de seu campus.

Seção II
Autenticação

Art. 8º A autenticação de usuários deve garantir que as pessoas ou sistemas que estão tentando acessar recursos ou informações sejam realmente quem afirmam ser.

§ 1º Um procedimento padronizado para autenticação de contas de usuário e serviços deve ser estabelecido, documentado e atualizado continuamente.

§ 2º Métodos apropriados de autenticação devem ser usados para controlar acesso de usuários remotos.

§ 3º Proteções contra ataques de força bruta, como bloqueios temporários de contas após um número específico de tentativas de login malsucedidas devem ser implementadas.

§ 4º Sempre que possível deve ser definida regras para expiração regulares das senhas.

§ 5º Sempre que possível, deve-se ativar a autenticação de dois fatores ou autenticação de múltiplos fatores.

§ 6º Os usuários devem seguir as boas práticas de segurança da informação na escolha e uso de senhas.

§ 7º Usuários devem utilizar senhas fortes, incluindo uma combinação de letras maiúsculas e minúsculas, números, caracteres especiais.

§ 8º O login e senha do usuário é de uso pessoal e intransferível, portanto é proibida sua divulgação ou compartilhamento, sob pena de serem bloqueados pela área de TI quando constatada qualquer irregularidade.

§ 9º Os usuários não devem compartilhar suas senhas com outras pessoas, mesmo com colegas de trabalho.

§ 10º Os usuários devem evitar o uso de informações pessoais óbvias, como nomes, datas de nascimento ou informações facilmente acessíveis na criação de senha.

§ 11º Os usuários não devem reutilizar senhas em diferentes contas ou serviços.

§ 12º Os usuários devem ser conscientizados sobre os riscos de segurança da informação relacionados ao uso de senhas e práticas seguras de gerenciamento de senhas.

Seção III
Autorização

Art. 9º A autorização de usuários deve determinar quais recursos ou informações um usuário específico está autorizado a acessar e em que extensão para garantir que apenas indivíduos autorizados obtenham acesso a dados ou recursos específicos.

§ 1º A concessão de acesso lógico deve estar em conformidade com as políticas, normas e procedimentos institucionais relativos à segurança da informação e privacidade de dados.

§ 2º Controles automatizados devem ser estabelecidos para a concessão e revogação de direitos de acesso.

§ 3º Rotinas devem ser definidas, documentadas e implementados para controlar a distribuição de direitos de acesso a recursos, sistemas de informação e serviços de TI.

§ 4º Os privilégios de acesso dos usuários a ativos/recursos de TI devem ser definidos pela área de TI conjuntamente com a área requisitante ao qual o usuário está vinculado, limitando-se a atividades estritamente necessárias à realização de suas tarefas.

§ 5º Sempre que possível deve ser aplicado o princípio do menor privilégio, concedendo aos usuários apenas as permissões e acessos necessários para desempenhar suas funções.

§ 6º Um procedimento padronizado para conceder e revogar acessos em todos os ativos, recursos, sistemas e serviços de TI deve ser estabelecido, documentado e atualizado continuamente.

§ 7º O acesso aos recursos, sistemas de informação e serviços de TI deve ser concedido e mantido pela área de TI, baseado nas responsabilidades, tarefas e funções de cada usuário.

§ 8º O nível de acesso aos ativos institucionais, recursos e serviços de TI deve ser realizado com base em perfis que definem o nível de privilégios dos usuários.

§ 9º O acesso à informações confidenciais e restritas deve ser configurado apenas quando uma necessidade de trabalho tiver sido identificada e tal acesso aprovado pelo setor responsável pela informação.

§ 10º Quando houver mudança do usuário para outro setor ou o usuário ocupar uma nova função, os direitos de acesso à rede local devem ser atualizados, conforme solicitação do responsável pelo setor.

§ 11º Os direitos de acesso de um usuário devem ser revisados periodicamente e ajustados de acordo com mudanças nos processos de negócios.

§ 12º Compete ao setor de gestão de pessoas da unidade solicitar a revogação de permissão de acesso do usuário aos recursos, sistemas e serviços de TI em caso de afastamentos, alterações de lotação, localização ou desligamentos.

§ 13º Os direitos de acesso de todos os servidores, estudantes, prestadores de serviços, fornecedores e terceiros às informações e aos recursos de processamento da informação deverão ser retirados após o encerramento de suas atividades, contratos ou acordos.

CAPÍTULO VI
DO MONITORAMENTO E AUDITORIA

Art. 10º As atividades de acesso dos usuários devem ser registradas e monitoradas para detectar atividades suspeitas ou não autorizadas e garantir a conformidade com as políticas de

segurança, identificar possíveis ameaças ou atividades suspeitas, e permitir uma análise detalhada das ações realizadas.

§ 1º Um procedimento padronizado para revisão e auditoria periódica dos *logs* de acesso deve ser estabelecido, documentado e mantido atualizado continuamente.

§ 2º Análise e controle de acesso aos ativos, recursos e serviços de TI devem ser realizadas em intervalos regulares para validar se todos os privilégios estão autorizados para a execução de atividades de cada função.

§ 3º Auditorias de tentativas de acesso aos ativos, recursos, sistemas e serviços de TI devem ser realizados em intervalos regulares para detectar atividades não autorizadas ou tentativas de comprometimento.

§ 4º O monitoramento e auditoria deve envolver:

I - o registro de atividades dos usuários;

II - a análise dos registros de atividades para identificar padrões incomuns ou atividades suspeitas;

III - configuração de alertas para notificar imediatamente a equipe de segurança sobre atividades suspeitas ou violações de políticas de acesso;

IV - realização de auditorias periódicas para revisar e avaliar os registros de atividades, garantindo conformidade com a política de segurança da informação e legislação pertinente; e

V - verificação regular dos privilégios de acesso dos usuários para garantir que estejam alinhados com suas funções atuais, evitando acessos desnecessários que possam representar riscos de segurança.

CAPÍTULO VII
DAS COMPETÊNCIAS, ATRIBUIÇÕES E RESPONSABILIDADES

Seção I
Da Alta Administração

Art. 11° Compete à alta administração:

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

II - garantir recursos (humanos, tecnológicos e financeiros) para a execução de ações relacionadas ao controle de acesso no âmbito do IFTO.

Seção II
Do Gestor de Tecnologia da Informação

Art. 12° Compete ao Gestor de Tecnologia da Informação:

I - planejar, implementar e melhorar continuamente os controles de acesso em soluções de tecnologia da informação e comunicações, nos termos da legislação vigente na Administração Pública Federal; e

II - propor diretrizes, competências e responsabilidades para a política, norma e processo de controle de acesso.

Seção III
Do Gestor de Segurança da Informação

Art. 13° Compete ao Gestor de Segurança da Informação:

I - coordenar a elaboração da política, norma interna complementar e processo de controle de acesso, observadas as normas afins exaradas pelo Gabinete de Segurança Institucional da Presidência da República;

II - assessorar a alta administração na implantação da política, normas interna complementar e processo de controle de acesso no IFTO;

III - incentivar estudos de novas tecnologias, bem como seus eventuais impactos relacionados à controle de acesso;

IV - propor recursos necessários às ações de controle de acesso;

V - verificar os resultados dos trabalhos de auditoria sobre a gestão de controle de acesso; e

VI - acompanhar a aplicação de ações corretivas e administrativas cabíveis nos casos relacionados à gestão de controle de acesso.

Seção IV
Do Comitê de Segurança da Informação

Art. 14° Compete ao Comitê de Segurança da Informação:

I - deliberar sobre política, norma interna complementar e processo de controle de acesso;

II - assessorar a implementação das ações de controle de acesso;

III - constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre controle de acesso;

IV - propor diretrizes, competências e responsabilidades para a política, norma interna complementar e processo de controle de acesso.

Seção V
Da Equipe de Tratamento e Resposta a Incidentes Cibernéticos

Art. 15° Compete à Equipe de Tratamento e Resposta a Incidentes Cibernéticos:

I - propor procedimento padronizado para o controle de acesso; e

II - propor diretrizes, competências e responsabilidades para a política, norma interna complementar e processo de controle de acesso.

Seção VI
Da Diretoria de Tecnologia da Informação e demais setores de Tecnologia da Informação nas unidades do IFTO

Art. 16° Compete à Diretoria de Tecnologia da Informação e demais setores de TI nas unidades do IFTO:

I - pesquisar, implantar e manter soluções para gestão de controle de acesso no âmbito do IFTO;

II - propor e gerenciar procedimentos de gestão de controle de acesso para a rede de comunicação de dados do IFTO;

III - definir, implementar e gerenciar um sistema de controle de acesso para os ativos de informação do IFTO;

IV - implantar, configurar, gerenciar e monitorar a estrutura de controle de acesso;

V - implementar rotinas para gestão de controle de acesso;

VI - prover o controle e a autenticação das conexões externas dos usuários e viabilizar a segurança da informação quando for necessária a utilização de computação móvel e demais recursos de trabalho remoto;

VII - analisar e auditar de forma crítica os direitos de acesso lógico dos usuários, em conformidade com legislação vigente, à política de segurança da informação e às boas práticas de segurança da informação;

VIII - divulgar e sensibilizar a política de controle de acesso lógico aos usuários ativos do IFTO;

IX - receber e analisar solicitações para criação de contas de acesso ou fornecimento de privilégios para usuários;

X - criar contas de usuários observando a premissa do menor privilégio possível, os requisitos do negócio e o resultado da análise de risco;

XI - conceder, quando autorizado, o acesso aos usuários, conforme indicado pelos gestores da informação;

XII - revogar, quando solicitado, o acesso dos usuários, conforme indicado pelos gestores da informação;

XIII - revisar periodicamente a validade de credenciais de acesso a ativos/sistemas de informação dos usuários fornecendo informações sobre os privilégios atualmente efetivados em ativos/sistemas de informação; e

XIV - propor diretrizes, competências e responsabilidades para a política, norma interna complementar e processo de controle de acesso.

Seção VII
Da Diretoria de Gestão de Pessoas e demais Setores de Gestão de Pessoas nas unidades do IFTO

Art. 17° Compete à Diretoria de Gestão de Pessoas e demais setores de Gestão de Pessoas nas unidades do IFTO:

I - comunicar a área de TI sobre desligamentos de servidores, prestadores de serviços, fornecedores, professores substitutos, voluntários, para que seja efetuado o bloqueio ou revogação da permissão de acessos aos recursos, sistemas de serviços de TI; e

II - propor diretrizes, competências e responsabilidades para a política, norma interna complementar e processo de controle de acesso.

Seção VIII
Dos Demais Setores

Art. 18° Compete aos demais setores:

I - informar a área de TI sobre a revogação de permissões de acesso à usuários vinculados a seu setor; e

II - propor diretrizes, competências e responsabilidades para a política, norma interna complementar e processo de controle de acesso.

Seção IX
Dos Usuários

Art. 19° Compete aos usuários:

I - atender aos princípios e diretrizes contidos nesta política, 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 - interromper a conexão aos sistemas e adotar medidas que bloqueiem o acesso de terceiros, sempre que completarem suas atividades ou quando se ausentarem do local de trabalho por qualquer motivo;

IV - informar ao setor de TI qualquer situação da qual tenha conhecimento que configure violação de sigilo ou que possa colocar em risco a segurança inclusive de terceiros;

V - zelar pelo uso dos sistemas informatizados, tomando as medidas necessárias para restringir ou eliminar riscos para o IFTO;

VI - não permitir a interferência externa caracterizada como invasão, monitoramento ou utilização de sistemas por terceiros, e outras formas;

VIII - não se conectar a sistemas e não buscar acesso a informações para as quais não lhe tenham sido dadas senhas e/ou autorização de acesso;

IX - utilizar corretamente os ativos de TI e conservá-los conforme os cuidados e medidas preventivas estabelecidas;

X - não divulgar suas senhas e nem permitir que terceiros tomem conhecimento delas, reconhecendo as como pessoais e intransferíveis;

XI - solicitar uma senha, quando do esquecimento;

XII - evitar o registro de senhas em qualquer meio;

XIII - alterar a sempre que existir qualquer indicação de possível comprometimento de sua confidencialidade;

XIV - criar senhas que sejam fáceis de lembrar, mas que não sejam baseadas em elementos que outras pessoas ou possíveis invasores possam facilmente adivinhar, ou deduzir, a partir de informações pessoais como por exemplo;

XV - alterar a senha em intervalos regulares e evitar a reutilização de senhas antigas;

XVI - selecionar senhas de boa qualidade, evitando o uso de senhas muito curtas ou muito longas, que o obrigue a registrá-la em qualquer outro meio para não serem esquecidas; e

XVII - encerrar as sessões ativas ou utilizar-se do mecanismo de bloqueio de acesso (tela de proteção com senha) quando precisar se afastar dos equipamentos, mesmo que seja por um período curto.

CAPÍTULO VIII
DAS PENALIDADES

Art. 20º Ações que violem esta política, norma interna complementar, procedimentos, ou que comprometem os controles de segurança da informação relacionados à controle de acesso 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 Qualquer utilização não autorizada ou tentativa de utilização não autorizada de credenciais e senhas de acesso a ativos/serviços de informação ou recursos computacionais será tratada como um incidente de segurança da informação, cabendo uma análise da infração

pela ETIR e aplicação das sanções e punições previstas na legislação pertinente à administração pública federal.

§ 2º Em situação em que haja suspeita de quebra da segurança da informação, colocando em risco os serviços ou recursos de tecnologia, a área de Tecnologia da Informação conduzirá a investigação, podendo interromper temporariamente o serviço afetado, sem prévia autorização.

§ 3º Nos casos em que o responsável pela violação de segurança for um usuário, a área de Tecnologia da Informação comunicará os resultados ao superior imediato do mesmo para adoção de medidas cabíveis.

§ 4º O procedimento para a aplicação das penalidades e/ou sanções seguirá o rito específico da legislação, norma, regimento ou resolução a que corresponder o caso concreto.

§ 5º Casos omissos não tratados neste documento serão submetidos, analisados, tratados e decididos pelo Comitê de Segurança da Informação.

CAPÍTULO IX
DA REVISÃO E ATUALIZAÇÃO

Art. 21° Esta política bem como norma interna complementar, processo, procedimentos e controles de acesso, devem passar por revisões, aprovações e atualizações sempre que houver alterações na legislação pertinente, nas diretrizes políticas do governo federal, alterações nas normativas internas do IFTO, ou quando considerada necessária pelo Comitê de Segurança da Informação.

CAPÍTULO X
DAS DISPOSIÇÕES FINAIS

Art. 22º Todo sistema de informação e serviços digitais, adquiridos ou desenvolvidos pelo IFTO a partir da publicação desta política deve priorizar o uso de controle de acesso conforme diretrizes estabelecidas nesta política.

Art. 23º Esta política e suas atualizações, bem como norma interna complementar, 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. 24º A alta administração deverá disponibilizar os recursos (humanos, tecnológicos e financeiros) necessários para a execução das diretrizes contidas nesta política.

Art. 25º Esta política entra em vigor na data de sua publicação.

Documento assinado eletronicamente por **Fabiana Ferreira Cardoso**, **Gestora de Segurança da Informação**, em 19/12/2023, às 10:42, 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 16:20, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

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 23235.004616/2023-04 SEI nº 2222401