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

PROCESSO DE CONTROLE DE ACESSO À INFORMAÇÃO E AOS ATIVOS ASSOCIADOS À INFORMAÇÃO

HISTÓRICO DE VERSÕES

Data	Versão	Descrição
04/01/2024	1	Elaboração do processo de controle de acesso à informação e aos ativos associados à informação.

1. INTRODUÇÃO

O controle de acesso de usuários é essencial para proteger informações confidenciais, garantir a segurança dos dados dos docentes, técnicos administrativos, estudantes, prestadores de serviços, estagiários, voluntários e visitantes do IFTO. O processo de controle de acesso à informação e aos ativos associados à informação refere-se à implementação de medidas de segurança para garantir que apenas usuários autorizados tenham acesso a informações e recursos específicos.

No IFTO este processo é realizado a partir da criação, provisionamento, uso e encerramento de contas e credenciais de usuários. Dentro deste contexto, este documento apresenta uma breve introdução, definições, controle de acesso à informação e aos ativos associados à informação, papéis e responsabilidades, matriz RACI, indicador de desempenho, práticas recomendadas e referências.

1.1. Escopo

Este processo compreende atividades coordenadas para proteger informações confidenciais, como dados pessoais, propriedade intelectual e segredos institucionais, garantindo, ao mesmo tempo que os usuários autorizados tenham acesso aos recursos necessários para desempenhar suas funções e atribuições.

1.2. Objetivos

O objetivo geral deste processo é garantir o acesso autorizado e impedir o acesso não autorizado a informações e outros ativos associados à informação. Para que este objetivo seja alcançado, são definidos os seguintes objetivos específicos:

a) segurança da Informação: assegurar que apenas usuários autorizados tenham acesso aos ativos de informação, protegendo-os contra acessos não autorizados, roubo de dados ou uso indevido;

b) confidencialidade: garantir que as informações sensíveis e confidenciais estejam protegidas contra acesso por pessoas não autorizadas, preservando sua privacidade e sigilo;

c) integridade dos dados: evitar alterações não autorizadas nos ativos de informação, mantendo sua integridade e precisão, protegendo contra modificações indevidas ou corrupção dos dados;

d) disponibilidade dos recursos: certificar-se de que os ativos de informação estejam disponíveis para os usuários autorizados quando necessário, garantindo que a informação crítica esteja acessível e utilizável;

e) conformidade com regulamentos: cumprir com requisitos legais, regulatórios e de conformidade aplicáveis à proteção de dados e informações sensíveis, evitando possíveis sanções ou penalidades;

f) redução de riscos: minimizar os riscos associados a possíveis ameaças internas e externas que poderiam comprometer a segurança ou a integridade dos ativos de informação;

g) gestão de identidades e acessos: gerenciar de forma eficiente identidades de usuários, suas permissões e privilégios de acesso para garantir que cada usuário tenha apenas as permissões necessárias para suas funções;

h) auditoria e rastreabilidade: possibilitar a monitorização e o rastreamento das atividades de acesso aos ativos de informação, permitindo a identificação de atividades suspeitas e a investigação em caso de incidentes;

i) educação e conscientização: promover a educação e a conscientização dos usuários sobre práticas seguras de acesso à informação, reduzindo potenciais vulnerabilidades decorrentes de falhas humanas; e

j) resposta a incidentes: estabelecer procedimentos para lidar com violações de segurança, incidentes de acesso não autorizado ou qualquer comprometimento dos ativos de informação.

1.3. **Abrangência**

O processo de controle de acesso à informação e aos ativos associados a informação é abrangente e deve ser aplicado em diversos níveis e áreas dentro de uma organização para garantir uma proteção efetiva dos dados e informações sensíveis. Sua abrangência geralmente engloba:

a) dados e informações: todos os tipos de dados e informações sensíveis, confidenciais ou críticas para a organização, independentemente de estarem em formato digital ou físico. Isso inclui dados pessoais, propriedade intelectual, estratégias comerciais, entre outros;

b) ativos de TI: todos os dispositivos, sistemas, redes, aplicativos, servidores e infraestrutura de TI que armazenam, processam ou transmitem informações. Isso abrange desde computadores e servidores até dispositivos móveis, impressoras e dispositivos de armazenamento;

c) usuários: todas as pessoas que interagem com os ativos de informação, incluindo servidores, prestadores de serviços, estiagiários, voluntários, parceiros comerciais, fornecedores e terceiros. O controle de acesso visa garantir que cada indivíduo tenha apenas as permissões necessárias para desempenhar suas funções;

d) locais físicos e remotos: o controle de acesso não se limita apenas a ambientes físicos, mas também se estende a acessos remotos, como conexões de rede, acesso via VPN (Rede Privada Virtual), acesso em nuvem, entre outros;

e) aplicações e sistemas: todos os sistemas, *softwares* e aplicativos utilizados para processar, armazenar ou transmitir dados devem ser protegidos por medidas de controle de acesso adequadas, incluindo controle de login, permissões de usuário e criptografia;

f) políticas e procedimentos: além das ferramentas tecnológicas, as políticas, procedimentos e diretrizes relacionados à segurança da informação são fundamentais para orientar as práticas de controle de acesso e definir padrões de uso seguro;

g) monitoramento e auditoria: a abrangência também inclui a implementação de sistemas de monitoramento e auditoria para registrar e rastrear atividades de acesso, garantindo a capacidade de revisar e analisar eventos de segurança; e

h) educação e conscientização: a conscientização dos usuários sobre práticas seguras de acesso à informação é parte integrante da abrangência do controle de acesso, visando reduzir riscos associados a falhas humanas.

1.4. **Benefícios esperados**

A execução eficaz do processo de controle de acesso à informação e aos ativos associados à informação oferece uma série de benefícios significativos para o IFTO, tais como:

a) segurança aprimorada: reduz o risco de acesso não autorizado a informações sensíveis, protegendo contra ameaças internas e externas, como hackers, ataques cibernéticos e vazamento de dados;

b) proteção da confidencialidade: garante que informações confidenciais e sigilosas sejam acessadas somente por pessoas autorizadas, preservando a privacidade e a confidencialidade dos dados;

c) integridade dos dados: evita alterações ou modificações não autorizadas nos ativos de informação, mantendo a precisão e a integridade dos dados ao longo do tempo;

d) conformidade regulatória: ajuda a cumprir regulamentações e padrões de conformidade e segurança, mitigando os riscos;

e) melhoria na gestão de riscos: identifica e reduz os riscos associados à segurança da informação, minimizando possíveis impactos negativos de violações de segurança;

f) eficiência operacional: atribui permissões e acessos de acordo com as necessidades individuais, permitindo que os funcionários realizem suas tarefas de forma mais eficiente e sem obstáculos desnecessários;

g) redução de incidentes de segurança: diminui a probabilidade de incidentes de segurança, como perda de dados, invasões e uso indevido de informações confidenciais;

h) melhoria na gestão de identidades: facilita o gerenciamento e a administração de identidades de usuários, atribuindo permissões adequadas a cada pessoa conforme suas responsabilidades;

i) aumento da consciência de segurança: promove uma cultura de segurança da informação entre os usuários, aumentando a conscientização sobre práticas seguras de uso e acesso aos dados; e

j) rastreabilidade e auditoria: permite o registro e monitoramento das atividades de acesso, fornecendo informações valiosas para auditorias de segurança e investigações em caso de incidentes.

2. DEFINIÇÕES

Para fins de compreensão dos termos utilizados neste processo serão utilizados os seguintes conceitos e definições:

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

b) 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;

c) 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;

d) ativo: tudo que tenha valor para a organização, material ou não;

e) ativos de informação: ativos com potencial para armazenar ou processar dados. Para fins deste documento, os ativos corporativos incluem dispositivos de usuário final, rede, não computacionais, internet das coisas e servidores em ambientes virtuais, baseados em nuvem e físicos;

f) ativos de software: são programas e outras informações operacionais usados em um ativo corporativo. Os ativos de software incluem sistemas operacionais e aplicações;

g) aplicação: programa, ou grupo de programas, hospedado em ativos corporativos e projetado para usuários finais. As aplicações são consideradas um ativo de *software* neste documento. Os exemplos incluem aplicações web, de banco de dados, baseadas em nuvem e móveis;

h) banco de dados: coleção organizada de dados, geralmente armazenados e acessados eletronicamente a partir de um sistema de computador. Os bancos de dados podem residir remotamente ou no local. Sistemas de gestão de banco de dados (SGBDs ou DMSs) são usados para administrar bancos de dados e não são considerados parte de um banco de dados para este documento;

i) 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;

j) 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;

k) 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;

l) 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;

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

n) conta de administrador: contas dedicadas com privilégios escalados e usadas para gerenciar aspectos de um computador, domínio ou toda a infraestrutura de tecnologia da informação da empresa. Os subtipos comuns de contas de administrador incluem contas root, contas de administrador local e de administrador de domínio e contas de administrador de rede ou dispositivos de segurança;

o) conta de usuário: identidade criada para uma pessoa em um computador ou sistema de computação. Para os fins deste documento, contas de usuário referem-se a contas de usuário "padrão" ou "interativas" com privilégios limitados e usadas para tarefas gerais, como ler e-mail e navegar na web. Contas de usuário com privilégios escalados são cobertas por contas de administrador;

p) contas de serviço: uma conta dedicada com privilégios escalados usada para executar aplicações e outros processos. As contas de serviço também podem ser criadas apenas para possuir dados e arquivos de configuração. Elas não se destinam ao uso por pessoas, exceto para a execução de operações administrativas;

q) 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;

r) CSI: Comitê de Segurança da Informação;

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

t) dispositivo remoto: Qualquer ativo corporativo capaz de se conectar a uma rede remotamente, geralmente da Internet pública. Isso pode incluir ativos corporativos, como dispositivos de usuário final, dispositivos de rede, dispositivos não computacionais/Internet das Coisas (IoT) e servidores;

u) documento: unidade de registro de informações, qualquer que seja o suporte ou o formato;

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

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

w) 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;

y) 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;

z) 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;

a1) 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;

b1) 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;

c1) incidente de segurança: qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

d1) informação: dados, processados ou não, que podem ser utilizados para produção e para transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

e1) internet: rede global, composta pela interligação de inúmeras redes;

f1) medidas de segurança: medidas destinadas a garantir sigilo, inviolabilidade, integridade, autenticidade e disponibilidade da informação classificada em qualquer grau de sigilo;

g1) política: intenções e diretrizes globais formalmente expressas pela direção;

h1) 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;

i1) 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;

j1) 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;

k1) recursos de processamento da informação: qualquer sistema de processamento da informação, serviço ou infraestrutura, ou as instalações físicas que os abriguem;

l1) 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;

m1) 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;

n1) segurança da informação: preservação da confidencialidade, integridade, disponibilidade, adicionalmente outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade, podem também estar envolvidas;

o1) serviços: refere-se a funcionalidade de software ou um conjunto de funcionalidades de software, como a recuperação de informações especificadas ou a execução de um conjunto de operações. Os serviços fornecem um mecanismo para permitir o acesso a um ou mais recursos, onde o acesso é fornecido usando uma interface determinada e com base na identidade do solicitante de acordo com as políticas de uso do IFTO;

p1) servidores: um dispositivo ou sistema que fornece recursos, dados, serviços ou programas a outros dispositivos em uma rede local ou em uma rede remota. Os servidores podem fornecer recursos e usá-los de outro sistema ao mesmo tempo. Os exemplos incluem servidores web, servidores de aplicações, servidores de e-mails e servidores de arquivos.

q1) SI: sigla de segurança da informação;

r1) 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;

s1) sistema operacional: software dos ativos corporativos que gerencia recursos de *hardware e software* do computador e fornece serviços comuns para programas. Os sistemas operacionais são considerados ativos de software e podem ser simples ou multitarefa, de um ou vários usuários, distribuídos, modelados, embarcados, em tempo real e biblioteca;

t1) 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

u1) 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.

3. CONTROLE DE ACESSO À INFORMAÇÃO E AOS ATIVOS ASSOCIADOS À INFORMAÇÃO

O controle de acesso à informação e aos ativos associados à informação no IFTO estabelece mecanismos para identificação, autenticação e autorização para salvaguardar as informações do IFTO, estejam elas em qualquer meio, seja digital ou físico. O objetivo é evitar a quebra da segurança da informação e qualquer acessos não autorizados que implique em risco de destruição, alteração, perda, roubo ou divulgação indevida.

O processo de controle de acesso à informação e aos ativos associados à informação refere-se a procedimentos realizados visando a segurança da informação na instituição. Dentre os diversos controles podem ser citados: senhas, biometria, criptografia, certificação e *hashing*.

3.1. Processo de controle de acesso à informação e aos ativos associados à informação

Segundo a UFV (2021), o processo de controle de acesso é crucial para garantir o uso de serviços à usuários autorizados e, ao mesmo tempo, prevenir que usuários não autorizados não tenham acesso à esses mesmos serviços. O processo de controle de acesso consiste em estabelecer fases e atividades para garantir que apenas as pessoas autorizadas tenham acesso aos recursos e informações confidenciais do IFTO. Isso envolve a implementação de medidas, envolvendo:

a) identificação de usuários: docentes, técnicos administrativos, estudantes, prestadores de serviços, estagiários, voluntários, visitantes são identificados através de informações pessoais, como nomes, números de identificação (matrícula/CPF/e-mail) etc;

b) autenticação de identidade: após a identificação, é necessária a autenticação para verificar a identidade do usuário. Isso pode ser feito através de diferentes métodos, como senhas, tokens, cartões de acesso, autenticação biométrica (impressão digital, reconhecimento facial etc.);

c) gerenciamento de credenciais: as credenciais de acesso (como senhas) precisam ser gerenciadas de forma segura. Isso inclui políticas de senha fortes, armazenamento criptografado e exigência de atualizações regulares de senha;

d) controle de acesso físico: importante para restringir quem pode entrar em determinadas áreas. Isso pode envolver o uso de cartões de acesso, leitores biométricos, câmeras de segurança, entre outros sistemas de controle;

e) controle de acesso lógico: realizado por meio de permissões de usuário, como níveis de acesso (administrador, professor, aluno), autenticação em duas etapas, firewalls, VPNs etc;

f) políticas de acesso e segurança: diretrizes sobre quem pode acessar quais recursos, como os dados devem ser protegidos, quais ações são permitidas e proibidas etc;

g) monitoramento e auditoria: detectar e responder a quaisquer tentativas de acesso não autorizado. Isso inclui logs de acesso, sistemas de detecção de intrusões e auditorias regulares para garantir conformidade com as políticas de segurança; e

h) educação e conscientização: treinamento regular dos usuários sobre práticas de segurança cibernética, importância de senhas fortes, reconhecimento de phishing etc., é fundamental para fortalecer a segurança do controle de acesso.

No IFTO o processo de controle de acesso à informação e aos ativos associados à informação é dividido em 3 (três) fases que auxiliam na proteção contra violação/vazamento de dados. A figura 1 apresenta o fluxo deste processo.

Figura 1 - Processo de controle de acesso à informação e aos ativos associados à informação

A tabela 1 apresenta a entrada, fases e saída do processo de controle de acesso.

Tabela 1 - Processo de controle de acesso à informação e aos ativos associados à informação

Processo de controle de acesso à informação e aos ativos associados à informação	
Entrada	Informações sobre o usuário.
Fases	1. Identificação. 2. Autenticação. 3. Autorização.
Saída	Informações.

3.1.1. Identificação

Fase responsável por reconhecer/identificar o usuário por meio da associação de uma solicitação de entrada a um conjunto de credenciais de identificação. Nesta fase poderão ser executadas as seguintes atividades:

a) registro de usuários e criação de perfis de acesso;

b) atribuição de credenciais de acesso únicas para cada identidade de usuário; e

c) identificação de usuário por meio de comparação de credenciais fornecidas às de um arquivo em um banco de dados de informações do usuário autorizado em um sistema operacional local, serviço de diretório de usuário ou em um servidor de autenticação.

3.1.2. Autenticação

Fase responsável por autorizar determinado usuário a acessar informações armazenadas nos ativos de TI. Exemplos de sistemas de autenticação podem incluir active directory, autenticação multifator (MFA), biometria e tokens. Nesta fase poderão ser executadas as seguintes atividades:

a) verificação de identidade do usuário por meio de métodos de autenticação, como autenticação multifatorial, biometria, autenticação de dois fatores entre outros; e

b) validação das credenciais de acesso por meio de diretório de controle de identidades.

3.1.3. Autorização

Fase responsável por autorizar determinado usuário a acessar informações armazenadas nos ativos de TI de acordo com os níveis de acesso ou privilégios de usuário/cliente relacionados aos recursos do sistema, incluindo arquivos, serviços, programas de computador, dados e recursos de aplicações. Um sistema de autorização concede ou nega acesso a um recurso com base na identidade do usuário. Exemplos de sistemas de autorização podem incluir active directory, listas de controle de acesso e lista de controle de acesso baseadas em funções. Nesta fase poderão ser executadas as seguintes atividades:

a) determinação do nível de acesso que o usuário terá no sistema, especificando quais permissão ele possui, como visualizar, editar, criar, fazer cópias e compartilhar;

b) verificação dos privilégios e permissões do usuário para garantir que correspondam ao nível apropriado de acesso aos ativos de informação, de acordo com suas funções e responsabilidades no IFTO; e

b) autorização do acesso à recursos, serviços e sistemas de informação com base nas permissões individuais de cada usuário.

4. PAPÉIS E RESPONSABILIDADES

Um papel é um conjunto de responsabilidades, atividades e autoridades definidas em um processo e atribuídas a uma pessoa, equipe ou função específica. No contexto no controle de acesso são definidos papéis e responsabilidades para cada ator envolvido no processo.

4.1. Alta Administração

Este papel representa o mais alto nível estratégico e decisório do IFTO, seja ela parte da administração pública federal. Compete ao representante deste nível as seguintes responsabilidades:

a) prover a orientação e o apoio necessário às ações de controle de acesso, de acordo com os objetivos estratégicos e com as leis e regulamentos pertinentes; e

b) disponibilizar os recursos (humanos, tecnológicos e financeiros) para a execução da política, norma interna complementar e processo de controle de acesso à informação e aos ativos associados à informação no âmbito do IFTO.

4.2. Comitê de Segurança da Informação

Este grupo de pessoas representam áreas finalísticas do IFTO. Compete a este grupo de pessoas a seguinte responsabilidade:

a) avaliar e aprovar a política, norma interna complementar e processo para controle de acesso à informação e aos ativos associados à informação.

4.3. Gestor de Segurança da Informação

Servidor(a) designado para gerir a segurança da informação. Compete à esta pessoa as seguintes responsabilidades:

a) propor a política, norma interna complementar e processo para gestão de controle de acesso à informação e aos ativos associados à informação;

b) elaborar e coordenar o processo de gestão de controle de acesso à informação e aos ativos associados à informação; e

c) designar um agente responsável pela execução das atividades referentes ao processo de controle de acesso à informação e aos ativos associados à informação, dentre os servidores efetivos do IFTO;

4.4. Equipe de Tratamento e Resposta a Incidentes Cibernéticos

Este grupo de pessoas é composto por servidores públicos civis ocupantes de cargo efetivo, com capacitação técnica compatível com as atividades dessa equipe. Compete à estas pessoas a seguinte responsabilidade:

a) avaliar a política, norma interna complementar, processo, plano, procedimentos e atividades sobre gestão de controle de acesso.

4.5. Setor de Tecnologia da Informação (Diretoria de Tecnologia da Informação e demais setores de TI das unidades do IFTO)

Agente responsável pela execução das atividades referentes ao processo de controle de acesso à informação e aos ativos associados à informação. Setor responsável por assegurar a execução da política, norma interna complementar, processo e atividades de controle de acesso no âmbito do IFTO. Neste sentido, compete a este setor as seguintes responsabilidades:

a) definir, implementar e gerenciar um sistema de controle de acesso para todos os ativos de informação do IFTO, não importando sua localização física;

b) disponibilizar ferramentas para gestão de usuários e controle de acesso lógico dos usuários;

c) 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;

d) estabelecer procedimentos que garantam a segurança da informação para o acesso aos sistemas informatizados;

e) buscar melhoria contínua para os processos de autenticação e controle de acesso lógico;

f) auxiliar as áreas de negócio na gestão de usuários, bem como fornecer treinamentos quando necessário;

g) 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;

h) divulgar e sensibilizar a política de controle de acesso aos usuários ativos do IFTO;

i) receber e analisar solicitações para criação de contas de acesso ou fornecimento de privilégios para usuários;

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

k) conceder, quando autorizado, o acesso aos usuários, conforme indicado pelos gestores da informação;

l) revogar, quando solicitado, o acesso dos usuários, conforme indicado pelos gestores da informação;

m) apoiar a revisão periódica da validade de credenciais de acesso a ativos/sistemas de informação dos usuários fornecendo informações sobre os privilégios atualmente efetivados em ativos/sistemas de informação;

n) prover a segurança da informação quando da utilização de programas utilitários que sejam capazes de sobrepor os controles dos sistemas e aplicações;

o) assegurar que o acesso à informação e às funções dos sistemas de aplicação, por parte do usuários, seja baseado nos requisitos de restrição de acesso do negócio; e

p) monitorar o acesso e o uso dos sistemas para os fins desta política.

4.6. Setor de Gestão de Pessoas

Setor responsável por informar a remoção de permissão nos sistemas de informação, recursos e serviços de TI. Compete a este setor a seguinte responsabilidade:

a) comunicar a área de TI sobre desligamentos de servidores, prestadores de serviços, professores substitutos, estagiários e voluntários, para que seja efetuado o bloqueio momentâneo ou revogação definitiva da permissão de acessos aos recursos, sistemas e serviços de TI.

4.7. Área de Negócio

Setor responsável por definir o direito de acesso dos usuários para os sistemas de informação relacionados a sua área de atuação. Compete ao setor

a seguinte responsabilidade:

a) informar a área de TI sobre a revogação de permissões de acesso à usuários vinculados a seu setor.

4.8. Usuário

Pessoa responsável por todos os acessos realizados através de sua conta de acesso e por possíveis danos causados à rede local e a recursos de tecnologia custodiados ou de propriedade do IFTO. Compete ao usuário as seguintes responsabilidades:

a) 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;

b) 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;

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

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

e) evitar sobrecarga de redes, de dispositivos de armazenamento de dados ou de outros, para não gerar indisponibilidade de informações internas e externas;

f) 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;

g) não divulgar a terceiros ou a outros usuários dispositivos ou programas de segurança existentes em seus equipamentos ou sistemas;

h) utilizar corretamente os equipamentos de informática e conservá-los conforme os cuidados e medidas preventivas estabelecidas;

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

j) manter a confidencialidade de sua senha pessoal;

k) trocar de senha na primeira vez que utilizar a conta de acesso aos sistemas e sempre suspeitar de invasão;

l) solicitar uma senha, quando do esquecimento;

m) evitar o registro de senhas em qualquer meio;

n) alterar a sempre que existir qualquer indicação de possível comprometimento de sua confidencialidade;

o) 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;

p) alterar a senha em intervalos regulares e evitar a reutilização de senhas antigas;

q) escolher suas próprias senhas;

r) 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

s) 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.

5. MATRIZ RACI

A matriz RACI apresentada na tabela 2 é utilizada para definir com clareza as atribuições, papéis e responsabilidades de cada colaborador nas atividades do processo. A sigla RACI significa, em inglês: *responsible, accountable, consulted e informed.*

a) ***responsible (responsável):*** pessoa, função ou unidade organizacional responsável pela execução de uma atividade no âmbito de um processo;

b) ***accountable (responsabilizado):*** dono da atividade, deverá fornecer os meios para que a atividade possa ser executada, e será responsabilizado caso a atividade não alcance os seus objetivos; cada atividade só pode possuir um *accountable*;

c) ***consulted (consultado):*** pessoas que deverão ser consultadas durante a execução da atividade; As informações levantadas junto a essas pessoas tornam-se entradas para a execução da atividade;

d) ***informed (informado):*** pessoas que serão informadas acerca do progresso da execução da atividade.

Tabela 2 - Matriz de responsabilidades

Fase	AA	CSI	GSI	ETIR	STI	SGP	AN	U
Identificação	A	C	C	C	R	I	I	I
Autenticação	A	C	C	C	R	I	I	I
Autorização	A	C	C	C	R	I	I	I

Legenda:

AA: Alta Administração.

CSI: Comitê de Segurança da Informação.

GSI: Gestor de Segurança da Informação.

ETIR: Equipe de Tratamento e Resposta a Incidentes Cibernéticos.

STI: Setor de Tecnologia da Informação (Diretoria de Tecnologia da Informação e demais Setor de Tecnologia da Informação das unidades IFTO).

SGP: Setor de Gestão de Pessoas.

AN: Área de Negócio.

U: Usuários.

6. INDICADOR DE DESEMPENHO

O processo de controle de acesso deve ser monitorado e medido através de indicador de desempenho. Esse indicador tem como objetivo acompanhar a eficácia do processo, identificando tendências, falhas e oportunidades de correções, promovendo sempre a melhoria contínua. A tabela 3 apresenta o indicador de desempenho deste processo.

Tabela 3 - Indicador de desempenho

Indicador	Número de recursos, serviços e sistemas que utilizam controle de acesso à informação.
Descrição	Quantificar os recursos, serviços e sistemas que utilizam controle de acesso à informação.
Objetivo	Gerenciar os recursos, serviços e sistemas que utilizam controle de acesso à informação.
Fonte	Catálogo de Serviços
Periodicidade	Anual.
Fórmula	Total de recursos, serviços e sistemas que utilizam controle de acesso à informação.
Meta	Aumentar o número de recursos, serviços e sistemas que utilizam controle de acesso à informação.

7. PROCESSOS RELACIONADOS

Para que a abordagem de segurança da informação seja efetiva, o processo de gestão de controle de acesso está interligado à outros processos que compõem o Sistema de Gestão de Segurança da Informação (SGSI-IFTO). A figura 2 apresenta estes processos.

Figura 2 - Processos que compõem o SGSI-IFTO

8. PRÁTICAS RECOMENDADAS

Para que este processo possa ser executado com eficiência faz-se necessária a observação das seguintes recomendações:

1. O IFTO deve instituir uma política de controle de acesso a qual estabelece princípios, objetivos, diretrizes, principais atividades e responsabilidades relativos ao processo de controle de acesso.

2. O IFTO deve estabelecer e manter um inventário dos sistemas de autenticação e autorização da organização, incluindo aqueles hospedados no site local ou em um provedor de serviços remoto. Revisar e atualizar o inventário anualmente ou com mais frequência.

3. O IFTO deve estabelecer e seguir um processo, de preferência automatizado, para conceder acesso aos ativos institucionais mediante nova contratação, concessão de direitos ou mudança de função de um usuário.

4. O IFTO deve manter um inventário dos ativos associados à informação e identificar as informações críticas que os ativos armazenam, processam ou transmitem.

5. O IFTO deve implementar controles de acesso físicos e lógicos à informação e aos ativos associados à informação que são por ela gerenciados ou custodiados, com vistas a proteger adequadamente a confidencialidade das informações não públicas e a integridade e a disponibilidade das informações consideradas críticas para o negócio.

6. O IFTO, quando possível deve implementar controles de acesso que aplicam o princípio ‘necessidade de conhecer’, o qual prescreve que deve haver necessidade legítima que justifique o acesso à informação por pessoa, sistema ou entidade, bem como o princípio ‘privilégio mínimo’, o qual estabelece que o perfil de acesso concedido deve incluir tão somente os poderes necessários para o atendimento das legítimas necessidades.

7. O IFTO, quando possível deve aplicar o modelo de segurança de ‘confiança zero’ (zero trust), o qual preconiza que uma identidade não é confiável até que seja adequadamente verificada para cada acesso pretendido, independentemente de perímetros.

8. Quando possível o IFTO analisa criticamente, a intervalos regulares, os direitos de acesso lógicos e físicos existentes, com vistas à remoção de direitos que deixaram de ser necessários e para assegurar que privilégios indevidos não foram obtidos.

9. O IFTO deve analisar criticamente, a intervalos regulares, os direitos de acesso lógicos e físicos existentes, com vistas à remoção de diretos que deixaram de ser necessários e para assegurar que privilégios indevidos não foram obtidos.

10. O IFTO deve avaliar periodicamente o desempenho e a conformidade do processo de controle de acesso à informação e aos ativos associados à informação e deve promover eventuais ajustes necessários.

11. Os controles de acesso implementados no IFTO sempre que possível devem aplicar o princípio "necessidade de conhecer", o qual prescreve que deve haver necessidade legítima que justifique o acesso à informação por pessoa, sistema ou entidade, bem como o princípio "privilégio mínimo", o qual estabelece que o perfil de acesso concedido deve incluir tão somente os poderes necessários para o atendimento das legítimas necessidades.

12. O IFTO deve sempre que possível utilizar controle de acesso lógico que utilizam autenticação com certificado digital, a fim de prover identificação inequívoca de pessoas físicas e jurídicas e comprovação de autoria em transações digitais.

13. O IFTO deve analisar criticamente de forma periódica os direitos de acesso lógicos e físicos existentes, com vistas à remoção de direitos que deixaram de ser necessários e para assegurar que privilégios indevidos não foram obtidos.

14. O IFTO deve avaliar periodicamente o desempenho e a conformidade do processo de controle de acesso à informação e aos ativos associados à informação e promover eventuais ajustes necessários.

15. O IFTO deve definir regras para o controle de acesso tomando-se como base os requisitos de acesso seguro a recursos, sistemas, softwares, aplicativos e serviços de TI.

16. 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.

17. Ferramentas/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*.

18. 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.

19. Quando possível o IFTO deve exigir que as aplicações corporativas ou de terceiros expostas externamente apliquem o MFA.

20. Quando possível o IFTO deve exigir MFA para acesso remoto à rede.

21. Quando possível o IFTO deve exigir MFA para todas as contas de acesso administrativo, em todos os ativos institucionais, sejam gerenciados no site local ou por meio de um provedor terceirizado.

22. Quando possível o IFTO deve centralizar o controle de acesso para todos os ativos institucionais por meio de um serviço de diretório ou provedor de SSO.

23. Quando possível o IFTO deve definir e manter o controle de acesso baseado em funções, determinando e documentando os direitos de acesso necessários para cada função dentro da organização para cumprir com sucesso suas funções atribuídas.

24. O IFTO deve realizar análises de controle de acesso de ativos institucionais para validar se todos os privilégios estão autorizados, em uma programação recorrente, uma vez por ano ou com maior frequência.

9. REFERÊNCIAS

UNIVERSIDADE FEDERAL DE VIÇOSA. **Processo de gestão de acesso.** Disponível em: https://www1.dti.ufv.br/wp-content/uploads/2021/05/11_gestao_de_acesso.pdf. Acesso em: 08/03/2023.

ANEXO I
Inventário de sistemas de autenticação

Ativo de Informação	Sistema de autenticação
E-mail Institucional	Google
Portal Institucional	Plone
Conferência Web	Rede CAFe

Eduplay	Rede CAFe
File Sender	Rede CAFe
Rede Wifi	Eduroam
SUAP	Diretório de autenticação de usuários.
SIGA-EPCT	Diretório de autenticação de usuários.
SEI	Diretório de autenticação de usuários.
Sistemas Integrados	Diretório de autenticação de usuários.
Sophia Biblioteca	Sophia
Moodle	Diretório de autenticação de usuários.

Documento assinado eletronicamente por **Fabiana Ferreira Cardoso**, **Gestora de Segurança da Informação**, em 05/01/2024, às 18:08, 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 **2237361** e o código CRC **D43BEC23**.

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