RESOLUÇÃO Nº 03, DE 19 DE MAIO DE 2023,

DO COMITÊ DE GOVERNANÇA DIGITAL

Aprova a Política de Controle de Acesso em Tecnologia da Informação e Comunicação do Instituto Federal de Educação, Ciência e Tecnologia de Santa Catarina.

O PRESIDENTE DO COMITÊ DE GOVERNANÇA DIGITAL DO INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SANTA CATARINA, no uso das atribuições que lhe foram conferidas pelo Art. 6º, inciso IV e Art. 9º, deste comitê.

RESOLVE:

Art. 1º Aprovar a Política de Controle de Acesso em Tecnologia da Informação e Comunicação;

Art. 2º Revogar a Resolução Nº 01/2021 do Comitê de Governança Digital;

Art. 3º Esta Resolução entra em vigor na data de 01 de junho de 2023.

gov.br
Documento assinado digitalmente
JESUE GRACILIANO DA SILVA
Data: 30/05/2023 21:03:37-0300
Verifique em https://validar.iti.gov.br

Jesué Graciliano da Silva
Presidente do Comitê de Governança Digital

Obs.: Súmula da reunião do CGD disponível em:
https://sigrh.ifsc.edu.br/sigrh/downloadArquivo?idArquivo=3130759&key=557b4380f5834be9bdfee8b450b25cad

POLÍTICA DE CONTROLE DE ACESSO EM TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

INSTITUTO FEDERAL
Santa Catarina

MINISTÉRIO DA EDUCAÇÃO

SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SANTA CATARINA

POLÍTICA DE CONTROLE DE ACESSO EM TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

Florianópolis - Junho/2023

COMITÊ DE GOVERNANÇA DIGITAL

Presidência

Jesué Graciliano da Silva
Pró-reitor de Desenvolvimento Institucional

Secretário-Executivo

Benoni de Oliveira Pires – Diretor de TIC

Membros do CGD

Titulares

Aloísio da Silva Júnior – Pró-reitor de Administração

Adriano Larentes da SIlva – Pró-reitor de Ensino

Valter Vander da Silveira – Pró-reitor de Extensão e Relações Externas

Flavia Maia Moreira – Pró-reitora de Pesquisa, Pós-Graduação e Inovação

Tiago Semprebom – Colégio de Dirigentes (São José)

Daniel Fernando Carossi – Colégio de Dirigentes (São Lourenço do Oeste)

Evaristo Marcos de Quadros Júnior – Encarregado do Tratamento dos Dados Pessoais

Suplentes

Eliana Cristina Bar – Colégio de Dirigentes (Palhoça)

José Roberto Machado – Colégio de Dirigentes (Jaraguá do Sul)

Equipe de Elaboração

Coordenador

Benoni de Oliveira Pires

Membros

Aline Pacheco Primão

Farleir Luís Minozzo

CAPÍTULO I

DO PROPÓSITO E ESCOPO

Art. 1º A Política de Controle de Acesso objetiva estabelecer controles de identificação, autenticação e autorização para salvaguardar as informações do Instituto Federal de Educação, Ciência e Tecnologia de Santa Catarina - IFSC, 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 implique em risco de destruição, alteração, perda, roubo ou divulgação indevida.

Art. 2º O crachá de identificação funcional e *login* de acesso aos sistemas de informações, são pessoais e intransferíveis e são o único método legítimo pelo qual o direito de acesso físico e/ou lógico podem ser exercidos.

Art. 3º Esta Política se aplica a todas as informações em que o IFSC seja o agente de tratamento, ao meio utilizado para este tratamento, seja digital ou físico, e as dependências físicas desta instituição, bem como a qualquer pessoa que circule nas dependências ou que interaja exercendo controle administrativo, técnico ou operacional, mesmo que eventual, desses meios de tratamento, incluindo:

I. Todos os colaboradores, sejam servidores efetivos (ativos e inativos) ou temporários do IFSC;
II. Todos os contratados e terceiros que trabalham para o IFSC;
III. Todos os funcionários de parceiros que acessam fisicamente as dependências ou que acessam a rede e sistemas de informação do IFSC;
IV. Todos os discentes com matrícula ativa no IFSC.

CAPÍTULO II

DOS TERMOS E DEFINIÇÕES

Art. 4º Termos e definições:

I. **2FA** - acrônimo para Autenticação de Dois Fatores (*2 Factor Authentication*);
II. **AUTENTICAÇÃO DE MULTIFATORES (MFA)** - utilização de dois ou mais fatores de autenticação para concessão de acesso a um sistema. Os fatores de autenticação se dividem em: algo que o

usuário conhece (senhas, frases de segurança, PIN, dentre outros); algo que o usuário possui (certificado digital, tokens, códigos enviados por SMS, dentre outros); algo que o usuário é (aferível por meios biométricos, tais como digitais, padrões de retina, reconhecimento facial, dentre outros); e onde o usuário está (quando o acesso só pode ser feito em uma máquina específica, cujo acesso é restrito);

III. **AUTORIZAÇÃO** - processo que ocorre após a autenticação e tem a função de diferenciar os privilégios atribuídos ao usuário que foi autenticado. Os atributos de autorização normalmente são definidos em grupos mantidos em uma base de dados centralizada, sendo que cada usuário herda as características do grupo a que ele pertence. Portanto, autorização é o direito ou permissão de acesso a um recurso de um sistema;

IV. **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;

V. **AUTO CADASTRO** - cadastro efetuado mediante ação do usuário;

VI. **BLOQUEIO DE ACESSO** - processo que tem por finalidade suspender temporariamente o acesso;

VII. **CADASTRO** - ação de inserção de dados de acesso em sistemas oficiais;

VIII. **CREDENCIAL (OU CONTA DE ACESSO)** - permissão, concedida por autoridade competente após o processo de credenciamento, que habilitam determinada pessoa, sistema ou organização ao acesso de recursos. A credencial pode ser física (como um crachá), ou lógica (como a identificação de usuário e senha);

IX. **CREDENCIAMENTO** - processo pelo qual o usuário recebe credenciais de segurança que concederão o acesso, incluindo a identificação, a autenticação, o cadastramento de código de identificação e definição de perfil de acesso em função de autorização prévia e da necessidade de conhecer;

X. **CREDENCIAMENTO DE SEGURANÇA** - processo utilizado para habilitar órgão ou entidade pública ou privada ou para credenciar pessoa, para o tratamento de informação classificada;

COMPROMETIMENTO - perda de segurança resultante do acesso não autorizado;

XI. **CONTA DE SERVIÇO** - conta de acesso à rede corporativa de computadores necessária a um procedimento automático (aplicação,script, etc) 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 DE ACESSO À INFORMAÇÃO CLASSIFICADA** - realizado através de credencial de segurança e da demonstração da necessidade de conhecer;

XIV. **CSIRT-IFSC** - Equipe de Tratamento e Resposta a Incidentes Cibernéticos do Instituto Federal de Educação;

XV. **DIREITO DE ACESSO** - privilégio associado a um cargo, pessoa ou processo para ter acesso a um ativo;

XVI. **DELEGAÇÃO DE ACESSO** - criação de acessos ou permissões delegadas a outros usuários;

XVII. **EXCLUSÃO DE ACESSO** - processo que tem por finalidade suspender definitivamente o acesso, incluindo o cancelamento do código de identificação e de perfil de acesso;

XVIII. **LISTA DE CONTROLE DE ACESSO (ACL)** - mecanismo que implementa o controle de acesso para um recurso enumerando as entidades do sistema que possuem permissão para acessar o recurso e definindo, explicitamente ou implicitamente, os modos de acesso concedidos à cada entidade;

XIX. **NÍVEIS DE ACESSO** - especificam quanto de cada recurso ou sistema o usuário pode utilizar;

XX. **PERFIL DE ACESSO** - conjunto de atributos de cada usuário, definidos previamente como necessários para credencial de acesso;

XXI. **PERFIL INSTITUCIONAL** - cadastro do órgão ou entidade da APF como usuário em redes sociais, alinhado ao planejamento estratégico e à PSI da instituição, com observância de sua correlata atribuição e competência;

XXII. **SETOR DESIGNADOR DE ACESSO** - No âmbito de câmpus é a Coordenadoria de Tecnologias da Informação e Comunicação ou Departamento de Tecnologia da Informação e Comunicação ou outro setor equivalente. Na Reitoria é a Diretoria de Tecnologias da Informação em conjunto com a Coordenadoria de Infraestrutura e Redes;

XXIII. **SETOR DESIGNADOR DE PERMISSÕES** - No âmbito do câmpus Coordenadoria de Gestão de Pessoas ou estrutura similar, e no âmbito da Reitoria é a Coordenadoria de Controle Funcional da Diretoria de Gestão de Pessoas ou estrutura que venha a substituir;

XXIV. **SETOR RESPONSÁVEL PELA GESTÃO DE PESSOAS** - No âmbito do Câmpus é a Coordenadoria de Gestão de Pessoas; no Câmpus Florianópolis é o Departamento de Gestão de Pessoas e na Reitoria é a Diretoria de Gestão de Pessoas.

XXV. **SETOR RESPONSÁVEL PELA GESTÃO DOS ACESSOS -** No âmbito do Câmpus é a Coordenadoria de Tecnologias da Informação e Comunicação, ou Departamento de Tecnologia da Informação e Comunicação ou outro setor equivalente. Na Reitoria é a Coordenadoria de Infraestrutura de Redes. Em relação ao SIG (Sistema de Gestão Integrado) os acessos aos módulos são de responsabilidade da diretoria responsável pelo mesmo.

XXVI. **SETOR RESPONSÁVEL PELA TECNOLOGIA DA INFORMAÇÃO** - No âmbito do IFSC, a Diretoria de Tecnologias da Informação e Comunicação do IFSC e coordenadorias vinculadas, são as Unidades Organizacionais responsáveis. De forma solidária, no âmbito dos câmpus, as Coordenadorias de Tecnologia da Informação e Comunicação ou Departamentos de Tecnologia da Informação e Comunicação são as Unidades Organizacionais responsáveis;

XXVII. **SETOR LOCAL DE SUPORTE EM TI -** No âmbito do Câmpus é a Coordenadoria de Tecnologias da Informação e Comunicação ou Departamento de Tecnologia da Informação e Comunicação ou outro setor equivalente. Na Reitoria é a Coordenadoria de Infraestrutura de Redes;

XXVIII. **SISTEMA DE ACESSO** - conjunto de ferramentas que se destina a controlar e a dar permissão de acesso a uma pessoa a um recurso;

XXIX. **SUBDELEGAÇÃO DE ACESSO** - Qualquer usuário que subdelega seu acesso mediante acesso programático, sendo vedada esta ação através do compartilhamento de senhas ou chaves de acesso;

XXX. **TERMO DE RESPONSABILIDADE** - termo assinado pelo usuário concordando em contribuir com a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações a que tiver acesso, bem como assumir responsabilidades decorrentes de tal acesso;

XXXI. **UORG -** No âmbito da Administração Pública significa Unidade Organizacional;

XXXII. **VÍNCULO INSTITUCIONAL** - Ligação a instituição denotada através de matrícula ou qualquer outro meio formal de atuação no âmbito interno da instituição;

XXXIII. **VPN -** Virtual Private Network (Rede Virtual Privada).

CAPÍTULO III

ACESSO LÓGICO

Art. 5º Todo usuário que vier a utilizar uma conta com controle de acesso deve ter ciência da Política de Segurança da Informação - PSI do IFSC e das normas estabelecidas na Política de Comunicação do IFSC.

Art. 6º O acesso lógico aos recursos dos Sistemas do IFSC, deve ser realizado por meio de sistema de controle de acesso. O acesso deve ser concedido e mantido pelo **setor responsável pela gestão dos acessos**, baseado nas responsabilidades e tarefas de cada usuário.

Art. 7º Terão direito a acesso lógico aos recursos dos Sistemas do IFSC os usuários de recursos de tecnologia da informação de toda comunidade do IFSC, sem distinção de público.

Art. 8º Consideram-se usuários de recursos de tecnologia da informação:

I. Servidores:

a) Docentes (ativos ou aposentados);

b) Técnicos-Administrativos (ativos ou aposentados);

c) Docentes substitutos.

II. Alunos:

a) de Pós-Graduação;

b) de Graduação;

c) de Nível Médio (médio, técnico e de jovens e adultos);

d) de Formação Inicial e Continuada.

III. Outros:

a) Tutor de Curso a Distância;

b) Responsável por entidade externa que utiliza o domínio do IFSC (procuradoria, grupos de pesquisa, e outros afins);

c) Entidade representativa de alunos;

d) Bolsistas;

e) Estagiários;

f) Servidores Terceirizados;

g) Visitantes;

Seção I

Do acesso à rede sem fio

Art. 9º O acesso através da Infraestrutura de Rede sem Fio do IFSC deverá ser organizado, segmentado e utilizado de forma compatível com os seguintes tipos de acesso:

I. Rede Administrativa: exclusiva para servidores efetivos, temporários ou estagiários e bolsistas;

II. Rede Discente: exclusiva para alunos do IFSC que estejam matriculados regularmente;

III. Rede *eduroam* é exclusiva para quem possui acesso pelo IFSC, para alunos, pesquisadores e visitantes de outras instituições de ensino e pesquisa que fazem parte do serviço internacional de provimento de rede sem fio denominado *"education roaming"*, serviço este mantido no Brasil pela Rede Nacional de Ensino e Pesquisa (RNP);

IV. Rede Visitante: exclusiva para funcionários de empresas terceirizadas que mantenham contrato vigente com o IFSC, alunos ou docentes de outras instituições que possuam convênio com o IFSC, representantes de empresas privadas ou instituições públicas em visita a Reitoria ou a algum câmpus do IFSC, participantes de eventos realizados na Reitoria ou em algum câmpus do IFSC;

a) As contas de usuários para a rede visitante poderão ser criadas na recepção da Reitoria ou dos câmpus ou no **SETOR LOCAL DE SUPORTE EM TI**.

b) As contas individuais da rede visitante deverão ter como "nome de usuário" o CPF da pessoa que irá usufruir da conta, sem pontos ou caracteres especiais seguido do @ifsc. Por exemplo, o CPF: 123.456.789-00 gerará um nome de usuário 12345678900@ifsc. A senha será gerada de forma aleatória pelo sistema de criação de contas.

c) Para eventos poderá ser criada uma única conta de usuário na rede visitante, sendo que o próprio nome do evento deverá fazer parte do nome de usuário. Para estes casos, é possível a definição de uma senha que seja fácil de memorizar.

d) O tempo de vida padrão para as contas definidas na rede visitante será de 24 horas. Havendo a necessidade de aumentar o tempo de vida padrão, a solicitação deve ser encaminhada:

I. Do **setor local de suporte em ti**, se a gerência da Infraestrutura de Rede sem Fio é centralizada na Reitoria do IFSC.

II. Diretamente para o **setor local de suporte em ti** do Câmpus, se a gerência da Infraestrutura de Rede sem Fio é descentralizada no IFSC.

Art. 10. O acesso remoto por meio de VPN (Rede Virtual Privada) deve ser evitado ao máximo, considerando a existência de novas tecnologias mais seguras como Zero Trust[1]. Quando utilizado, deve ser realizado único e exclusivamente para acesso por profissionais devidamente autorizados pela equipe de Tecnologia da Informação no âmbito do Campus ou da Reitoria.

Seção I

Dos direitos à conta de acesso com e-mail

Art. 11. Deverá possuir conta de acesso com e-mail:

I. Servidor efetivo ou temporário;

II. Todo setor presente nos organogramas dos câmpus e da Reitoria (UORGs), cujo acesso será prerrogativa do responsável pelo setor.

Art. 12. Poderá ter direito a conta de acesso com e-mail:

I. Toda pessoa que possua relação direta e vínculo ativo com o IFSC: discente, estagiário, bolsista externo, bolsista voluntário etc;

II. Todo servidor inativo;

[1] O modelo de segurança de confiança zero, também conhecido como arquitetura de confiança zero, arquitetura de rede de confiança zero ou acesso à rede de confiança zero, e às vezes conhecido como segurança sem perímetro, descreve uma abordagem para o projeto e implementação de sistemas de TI.

III. Todo colaborador contratado (terceirizado) pelo IFSC;

IV. Colabor externo com vínculo em algum programa institucional nas áreas de ensino, pesquisa e extensão;

V. Eventos e programas institucionais oficiais de ensino, pesquisa ou extensão, cujo acesso será prerrogativa do responsável e que poderão ser desativados mediante solicitação;

VI. Comissões, comitês e grupos de trabalho, desde que formalmente constituídos mediante Portaria;

VII. Entidades de representação estudantil, desde que legalmente constituídas e vinculadas ao IFSC;

VIII. Empresas juniores, desde que legalmente constituídas e vinculadas ao IFSC;

IX. Demais iniciativas institucionais avaliadas mediante solicitação ao **setor responsável pela tecnologia da informação**.

Art. 13. A solicitação para criação de e-mail dar-se-á das seguintes formas:

I. De forma automatizada para servidores efetivos, temporários e estagiários, a partir do cadastramento pelo setor responsável pela gestão de pessoas do IFSC;

II. De forma automatizada para alunos, a partir da matrícula e cadastramento no Portal Discente - SIGAA;

III. A partir de solicitação do gestor ou fiscal de contrato, no caso de e-mails para colaboradores contratados (terceirizados), e que terá sob sua responsabilidade a solicitação de desativação da conta após o encerramento do contrato;

IV. A partir de solicitação do diretor de ensino, pesquisa e extensão ou cargo equivalente ou ainda do coordenador de ensino/pesquisa/extensão, no caso de e-mails para colaboradores externos, e que terá sob sua responsabilidade a solicitação de desativação da conta após o encerramento da colaboração;

V. A partir de solicitação das assessorias das direções gerais dos câmpus ou pró-Reitorias, no caso de e-mails setoriais, quando da oficialização do setor/UORG;

VI. A partir de solicitação do servidor formalmente responsável pela supervisão, no caso de e-mails de tutores e bolsistas;

VII. A partir de solicitação do diretor de pesquisa ou extensão do câmpus ou equivalente, no caso de empresas juniores;

VIII. A partir de solicitação do diretor de ensino do câmpus ou equivalente, no caso de entidades de representação estudantil;

IX. A partir de um membro constante na portaria de criação, no caso de comissão ou grupo de trabalho, permanente ou temporária;

X. Para demais e-mails específicos do câmpus, deve ser solicitado ao responsável diretamente ao **setor local de suporte em ti** através da abertura de chamado (chamados.ifsc.edu.br ou enviando e-mail para suporte.ti.sigla-do-campus@ifsc.edu.br);

XI. Para casos não contemplados anteriormente, devem ser solicitados para a Diretoria de Tecnologias da Informação e Comunicação através da abertura de chamado (chamados.ifsc.edu.br ou enviando e-mail para suporte.ti@ifsc.edu.br).

Parágrafo único. As solicitações descritas nos incisos III a IX do caput deste artigo serão endereçadas ao setor local de suporte em TI de acordo com a abrangência do e-mail a ser criado.

Seção II

Do acesso às contas não pessoais

Art.14. Na utilização dos e-mails setoriais ou qualquer outra conta que não seja criada para utilização de pessoa física (que possua CPF), o acesso deverá ser feito mediante delegação.

I. As contas setoriais deverão ser acessadas através da delegação de acesso. É vedado o compartilhamento de senha para outros usuários, cabendo penalização em nível administrativo ao do titular do setor;

II. É de responsabilidade do solicitante da conta ou do responsável pelo setor, cadastrar seu endereço e de até outros (até o limite de 24 delegados) para acesso a conta de e-mail;

III. Não é possível acessar contas delegadas através de clientes de e-mails de terceiros, mas somente através do servidor oficial de e-mails do IFSC na sua versão web disponível para computadores;

IV. A delegação de conta deve ser feita pelo responsável ou seu superior imediato, inclusive em períodos de férias ou ausência do servidor delegado.

Seção III

Do bloqueio, desbloqueio e cancelamento da conta de acesso

Art. 15. Não terão direito a manter suas contas de e-mail no IFSC:

I. servidores exonerados, demitidos e redistribuídos;

II. servidores temporários ou substitutos com contrato encerrado (ou findado);

III. alunos que não tenham matrícula ativa no IFSC (curso concluído ou matrícula cancelada);

IV. estagiários, bolsistas externos e tutores com contrato encerrado;

V. colaboradores contratados com contrato encerrado;

VI. colaboradores externos com colaboração encerrada.

§1º. Ao findar o vínculo da pessoa com o IFSC, sua caixa postal e os dados armazenados serão mantidos acessíveis por 30 (trinta) dias corridos para que seja possível ao usuário fazer cópia de segurança dos dados e, após este prazo, a conta será desativada.

§2º. Quando solicitado por órgãos de controle externo, pela Assessoria de Correição do IFSC, por autoridade responsável por Processo Administrativo Disciplinar (PAD) ou por determinação do Reitor(a), referendado pela Procuradoria Geral da República, os acessos deverão ser revogados dentro do prazo estabelecido por estes.

Art. 16. Poderá o servidor, no momento da inatividade, fazer o redirecionamento dos e-mails @ifsc.edu.br para um endereço de e-mail particular mediante configuração manual.

Art. 17. Quando a impossibilidade de expansão de infraestrutura própria de armazenamento de dados ou políticas de serviços gratuitos de terceiros impuserem a necessidade de limitação de uso:

I. Serão definidas cotas para os usuários;

II. Será impossibilitado novos armazenamentos (upload de dados);

III. Contas de e-mail sem acesso superior a 30 dias serão desativadas sem aviso prévio.

Art. 18. Quando do afastamento do usuário (servidor público) para exercício em outro órgão público:

I. O acesso aos sistemas deverá ser bloqueado;

II. Perfis de acesso de ocupantes de cargos de gestão deverão ser retirados (mantendo o perfil básico);

III. O acesso ao e-mail e demais serviços vinculados deverão ser bloqueados;

§1º O desbloqueio se dará quando do retorno do servidor público.

§2º O setor responsável pela gestão de pessoas deverá informar a DTIC sobre a cessão do servidor a outro órgão.

Seção IV

Do acesso à listas de e-mail

Art. 19. As listas de e-mails institucionais poderão ser criadas a pedido de qualquer servidor do IFSC, mediante solicitação formal devidamente instruída com as razões e fundamentos institucionais que justifiquem a criação do grupo.

§1º A criação das listas ou grupos e-mails, quando autorizadas, serão moderadas pelas autoridades/setores nominados no Anexo III desta Política. A moderação das listas poderá ser delegada para outros usuários, ou mesmo indicar que os e-mails poderão ser entregues sem qualquer tipo de moderação. Quando houver a moderação, os remetentes das mensagens rejeitadas deverão receber uma justificativa para o seu não envio à lista.

§2º Todas as listas do IFSC são de responsabilidade de seus administradores e devem ser utilizadas como canal de relacionamento entre os servidores que delas fazem parte, para fins institucionais.

§3º Quando houver a moderação, os remetentes das mensagens rejeitadas deverão receber uma justificativa para o seu não envio à lista. Os critérios para envio de mensagens às listas são “Abrangência” e “Pertinência”, onde deve ser observado que a mensagem seja do interesse da maioria dos membros da lista e trate de assuntos relativos a processos e eventos do IFSC, respectivamente.

Art. 20. Os e-mails oriundos de contas especificadas no Anexo III e enviados para todas as listas, não serão moderados, podendo tratar de avisos, convocações, notícias, comunicações relacionadas com o sistema de informação da Instituição e todos os assuntos considerados de interesse institucional.

Seção V

Da conta de acesso lógico e senha

Art. 21. Para utilização das estações de trabalho do IFSC, será obrigatório o uso de uma única identificação (login) e senha de acesso, fornecidos exclusivamente através de meios pré-estabelecidos pelo **setor responsável pela gestão dos acessos**, mediante procedimento de criação de conta, quando do início do vínculo do usuário no IFSC.

I. Os privilégios de acesso dos usuários aos Sistemas do IFSC devem ser definidos pela unidade requisitante ao qual o usuário está vinculado, limitando-se a atividades estritamente necessárias à realização de suas tarefas.

II. Na necessidade de utilização de perfil diferente do disponibilizado, o titular da unidade do usuário(a) deverá encaminhar solicitação para o setor **responsável pela gestão de acessos** que a examinará, podendo negá-la com justificativas técnicas e/ou de segurança da informação.

III. Em relação ao SIG (SIPAC, SIGAA e SIGRH) os privilégios de acesso deverão ser dados pelas áreas de administração, ensino, pesquisa e extensão, a qual o usuário(a) esteja vinculado(a).

Art. 22. O login e senha são de uso pessoal e intransferível, sendo proibida a sua divulgação, sob pena de serem bloqueados pelo **responsável pela gestão de acessos** quando constatada qualquer irregularidade.

Parágrafo único. Para retomar o acesso à rede, deverá ser formalizada nova requisição pelo titular da unidade do requisitante.

Art. 23. O padrão adotado para o formato da conta de acesso do usuário é a sequência primeiro nome + ponto + último nome do usuário, como por exemplo, *joao.silva*, ou conforme disposto no ANEXO I desta política.

§1º As contas de acesso, grupos e listas criadas antes desta política e que diferem do formato definido, não sofrerão alteração;

Art. 24. A formação da senha da identificação (login) de acesso aos computadores e Sistemas do IFSC deve seguir as regras de:

I. Tamanho mínimo de oito caracteres, sendo obrigatório o uso de letras e números.

II. Utilização de letras maiúsculas, minúsculas e caracteres especiais ($, %, &,...);

III. Não ser formada por sequência numérica (123...), alfabética (abc...), nomes próprios, palavras de fácil dedução, datas, placa de carro, número de telefone, a própria conta de acesso, apelidos ou abreviações;

IV. Não utilizar termos óbvios, tais como: Brasil, senha, usuário, password ou system.

V. Não reutilizar as últimas [05 (cinco)] senhas.

Art. 25. O **SETOR RESPONSÁVEL PELA GESTÃO DE ACESSOS** fornecerá uma senha gerada aleatoriamente para cada conta de acesso criada no momento da liberação dessa conta e a mesma poderá ser alterada pelo usuário mantendo o padrão citado no art. 20 e seus incisos.

Art. 26. As senhas de acesso deverão ser renovadas anualmente, devendo o usuário ser informado ao acessar os sistemas, a fim de que ele próprio efetue a mudança.

Seção VI

Da conta de acesso biométrico

Art. 27. A conta de acesso biométrico, quando implementada, deve ser vinculada a uma conta de acesso lógico e ambas devem ser utilizadas para se obter um acesso, a fim de atender os conceitos da autenticação de multifatores.

Parágrafo único. O IFSC deverá tratar seus respectivos dados biométricos como dados sigilosos, preferencialmente, utilizando-se de criptografia, na forma da legislação vigente.

CAPÍTULO IV
MOVIMENTAÇÃO INTERNA

Art. 28. Quando houver mudança do usuário para outro setor ou Campus, os direitos de acesso à rede de dados devem ser readequados, conforme solicitação do novo superior imediato ou do **setor responsável pela gestão de pessoas**.

§1º Os direitos de acesso antigos devem ser imediatamente cancelados conforme solicitação do antigo superior imediato ou do **setor responsável pela gestão de pessoas**.

§2º Eventuais participações em listas de e-mails, grupos ou demais ferramentas locais, devem ser revogadas pelo administrador das mesmas.

CAPÍTULO V
ADMINISTRADORES

Art. 29. A utilização de identificação (login) com acesso no perfil de administrador é permitida somente para usuários cadastrados para execução de tarefas específicas na administração de ativos de informação. O acesso deve ser fornecido mediante atribuição de permissões, evitando assim identificadores (logins) não nominais ou desvinculados de pessoas físicas, que causariam a perda de rastreabilidade e auditoria.

Art. 30. Somente os profissionais de TIC do **setor responsável pela tecnologia da informação**, devidamente identificados e habilitados, terão usuários com privilégios de administrador nos equipamentos locais e na rede.

I. Na necessidade de utilização de login com privilégio de administrador do equipamento local, o usuário deverá encaminhar solicitação para o **setor responsável pela tecnologia da informação**, que poderá negar os casos em que entender desnecessária a utilização.

II. Se concedida a permissão ao usuário como administrador local na estação de trabalho, esse será responsável por manter a integridade da máquina, não podendo instalar, desinstalar ou

remover qualquer programa sem consulta prévia ao **setor responsável pela tecnologia da informação**.

III. Caso constatada a irregularidade, o usuário perderá o acesso como administrador, não mais podendo requerer outra permissão.

IV. A identificação (login) com privilégio de administrador nos equipamentos locais será fornecida em caráter provisório, podendo ser renovada por solicitação formal do titular da unidade requisitante.

V. Salvo para atividades específicas da área responsável pela gestão da tecnologia da informação do órgão, não será concedida, para um mesmo usuário, identificação (login) com privilégio de administrador para mais de uma estação de trabalho, ou para acesso a equipamentos servidores e a dispositivos de rede.

VI. Excepcionalmente, poderão ser concedidas identificações (login) de acesso à rede de comunicação de dados a visitante em caráter temporário após apreciação do **setor responsável pela tecnologia da informação** por meio do setor **responsável pela gestão dos acessos**.

Parágrafo único. O disposto no caput deste artigo, bem como em seus incisos não cabe aos computadores de uso pedagógico em laboratórios de informática, redes de computadores, desenvolvimento de sistemas e afins, cuja responsabilidade será da coordenação do curso a que estejam vinculados estes laboratórios;

CAPÍTULO VI

RESPONSABILIDADES

Art. 31. É de responsabilidade do **setor responsável pela gestão de pessoas** comunicar formalmente ao **setor responsável pela tecnologia da informação** o desligamento ou saída do usuário (servidor público) do IFSC, para que as permissões de acesso aos sistemas sejam canceladas.

Art. 32. Caberá ao **titular do acesso às contas de e-mail setoriais** efetuar delegação de acesso durante seu período de férias ou licenças planejadas.

Art. 33. É responsabilidade do **setor responsável pela gestão de mão-de-obra terceirizada** do IFSC a comunicação imediata ao **setor responsável pela tecnologia da informação** sobre desligamentos, férias e licenças de funcionários de empresas prestadoras de serviços, para que seja efetuado o bloqueio momentâneo ou revogação definitiva da permissão de acesso aos recursos.

Art. 34. É de responsabilidade do **setor responsável pela tecnologia da informação** o monitoramento da utilização de serviços de rede e de acesso à Internet, podendo ainda exercer fiscalização nos casos de apuração de uso indevido desses recursos, bem como bloquear, temporariamente, sem aviso prévio, a estação de trabalho que esteja realizando atividade que coloque em risco a segurança da rede, até que seja verificada a situação é descartada qualquer hipótese de dano à infraestrutura tecnológica do Instituto Federal de Santa Catarina.

Art. 35. O usuário é responsável por todos os acessos realizados através de sua conta de acesso e por possíveis danos causados aos Sistemas do IFSC e a recursos de tecnologia custodiados ou de propriedade do Instituto Federal de Santa Catarina.

I. O usuário é responsável pela integridade e utilização de sua estação de trabalho, devendo, no caso de sua ausência temporária do local onde se encontra o equipamento, bloqueá-lo ou desconectar-se da estação, para coibir acessos indevidos, mesmo quando em trabalho remoto.

II. A utilização simultânea da conta de acesso aos Sistemas do IFSC em mais de uma estação de trabalho ou notebook deve ser evitada, sendo responsabilidade do usuário titular da conta de acesso os riscos que a utilização paralela implica.[2]

III. O usuário não poderá, em hipótese alguma, transferir ou compartilhar com outrem sua conta de acesso e respectiva senha ou eventuais códigos de acesso aos Sistemas do IFSC

Art. 36. O usuário deve informar à Equipe de Tratamento e Respostas a Incidentes Cibernéticos (csirt@ifsc.edu.br) qualquer situação da qual tenha conhecimento que configure violação de sigilo ou que possa colocar em risco a segurança inclusive de terceiros.

[2] Sistemas modernos de segurança coíbem ações simultâneas de distâncias que caracterizem uma “viagem impossível”, bloqueando assim tentativas de acessos simultâneos.

Art. 37. É dever do usuário zelar pelo uso dos sistemas informatizados, tomando as medidas necessárias para restringir ou eliminar riscos para a instituição, a saber:

I. Não permitir a interferência externa caracterizada como invasão, monitoramento ou utilização de sistemas por terceiros, e outras formas;

II. Evitar sobrecarga de redes, de dispositivos de armazenamento de dados ou de outros, para não gerar indisponibilidade de informações internas e externas;

III. Interromper a conexão aos sistemas e adotar medidas que bloqueiem o acesso de terceiros, sempre que completar suas atividades ou quando se ausentar do local de trabalho por qualquer motivo;

IV. 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;

V. Não divulgar a terceiros ou a outros usuários dispositivos ou programas de segurança existentes em seus equipamentos ou sistemas;

VI. Utilizar corretamente os equipamentos de informática e conservá-los conforme os cuidados e medidas preventivas estabelecidas;

VII. Não divulgar suas senhas e nem permitir que terceiros tomem conhecimento delas, reconhecendo-as como pessoais e intransferíveis;

CAPÍTULO VII

DISPOSIÇÕES GERAIS

Art. 38. Os incidentes que afetem a Segurança das Informações, assim como o descumprimento da Política de Segurança da Informação e Normas de Segurança devem ser obrigatoriamente comunicados pelos usuários à Equipe de Tratamento e Respostas a Incidentes Cibernéticos (csirt@ifsc.edu.br).

Art. 39. Quando houver suspeita de quebra da segurança da informação que exponha ao risco os serviços ou recursos de tecnologia, a Equipe de Tratamento e Respostas a Incidentes Cibernéticos fará a investigação, podendo interromper temporariamente o serviço afetado, sem prévia autorização.

I. Nos casos em que o autor da quebra de segurança for um usuário, a Equipe de Tratamento e Respostas a Incidentes Cibernéticos comunicará os resultados ao superior imediato do mesmo para adoção de medidas cabíveis.

II. A resolução de casos de violação/transgressões omissas nas legislações correlatas será apreciada pelo **Comitê de Governança Digital do IFSC**.

Art. 40 A DTIC reserva-se no direito de adicionar requisitos, funcionalidades ou níveis de autorização e formas de acesso mais seguros, seja por oportunidade, correção ou quando resultar em aprimoramento do nível de segurança.

CAPÍTULO VIII

DISPOSIÇÕES FINAIS

Art. 41. Esta resolução deverá estar publicada em portal institucional e disponível para acesso e conhecimento de todos os usuários do IFSC.

Art. 42. É de responsabilidade de todos os usuários dos recursos de tecnologia da informação e comunicação ofertados pelo do IFSC tomarem conhecimento das normas de controle de acesso contidas nesta política.

Art. 43. Os casos omissos serão analisados pela Diretoria de Tecnologia da Informação e Comunicação.

ANEXO I

FORMATO DE CONTA DE ACESSO PESSOAL

O formato do endereço de conta de acesso pessoal é baseado no nome completo do indivíduo.

1. Exemplos de formação para Servidores:
   João da Silva Santos poderá escolher uma das opções apresentadas pelo sistema:
   joao.santos@ifsc.edu.br,joao.s.santos@ifsc.edu.br,
   joao.dasilva.santos@ifsc.edu.br,
   joao.dasilva@ifsc.edu.br,
   joao.silva@ifsc.edu.br,
   joao.santos2@ifsc.edu.br.

2. Exemplos de formação para Alunos:
   João Carlos dos Santos que nasceu em 01/02/1990, poderá escolher uma das opções apresentadas pelo sistema:
   joao.s@aluno.ifsc.edu.br
   joao.c@aluno.ifsc.edu.br
   joao.cs@aluno.ifsc.edu.br
   joao.s01@aluno.ifsc.edu.br,
   joao.s1990@aluno.ifsc.edu.br,
   joao.c01@aluno.ifsc.edu.br,
   joao.c1990@aluno.ifsc.edu.br,
   joao.cs01@aluno.ifsc.edu.br,
   joao.cs1990@aluno.ifsc.edu.br.

2.1. Se da lista acima, após verificação no sistema e exclusão das opções que já existirem, não restarem ao menos cinco (05) opções, o sistema adiciona incrementalmente um número às combinações com nome e sobrenome até haver ao menos cinco (05) opções de escolha:

joao.s2@aluno.ifsc.edu.br,
joao.c2@aluno.ifsc.edu.br,
joao.cs2@aluno.ifsc.edu.br,
joao.s10@aluno.ifsc.edu.br,
joao.c10@aluno.ifsc.edu.br,
joao.cs10@aluno.ifsc.edu.br.

ANEXO II
FORMATO DE CONTA DE ACESSO SETORIAL

Para contas setoriais, deve-se adotar o padrão e as siglas utilizadas devem seguir o padrão da Instrução Normativa nº 04 de 09 de Março de 2020[3].

Nome do Setor	Modelo de conta de acesso setorial
Direção-geral do câmpus	direcao.sigladocampus@
Diretoria/Departamento de Ensino, Pesquisa e Extensão	depe.sigladocampus@
Departamento/Coordenadoria de Assuntos Estudantis	dae.sigladocampus@ - para caso o câmpus tenha departamento assuntosestudantis.sigladocampus@ - para caso o câmpus tenha coordenadoria
Coordenadoria de Registro Acadêmico	ra.sigladocampus@
Coordenadoria de Secretaria Acadêmica	secretaria.sigladocampus@
Coordenadoria de Extensão	extensao.sigladocampus@
Coordenadoria Pedagógica	pedagogico.sigladocampus@
Coordenadoria de Biblioteca	biblioteca.sigladocampus@
Coordenadoria do Núcleo de Educação a Distância	nead.sigladocampus@
Coordenadoria de Pesquisa	pesquisa.sigladocampus@
Coordenadoria de Pós-graduação	pos.sigladocampus@
Coordenadorias de Cursos	**Cursos FIC:** nomedocurso.fic.sigladocampus@ **Cursos Técnicos:** nomedocurso.tec.sigladocampus@ **Cursos de Graduação:** **Licenciaturas**

[3] Acessível pelo endereço:
<https://intranet.ifsc.edu.br/index.php?option=com_content&task=view&id=1454&Itemid=637>.

	nomedocurso.lic.sigladocampus@ **Tecnólogos** nomedocurso.cst.sigladocampus@ **Bacharelados** nomedocurso.grad.sigladocampus@ ou nomedocurso.sigladocampus@ **Engenharias** eng.nomedocurso.sigladocampus@ **Cursos de Pós-Graduação:** nomedocurso.esp.sigladocampus@ nomedocurso.mestrado.sigladocampus@ nomedocurso.doutorado.sigladocampus@ ***Caso o curso seja ofertado em mais de um câmpus e haja uma coordenadoria apenas, utiliza-se por padrão:** nomedocurso.modalidade@
Coordenadoria de Inovação	inovacao.sigladocampus@
Coordenadoria de Relações Externas	relacoesexternas.sigladocampus@
Coordenadoria de Relações Externas e Extensão	cere.sigladocampus@
Coordenadoria de Relações Externas e Extensão e Comunicação	cere.sigladocampus@
Coordenadoria ou Setor de Comunicação Social	comunicacao.sigladocampus@
Coordenadoria de Estágios	estagio.sigladocampus@
Coordenadoria de Ingresso	ingresso.sigladocampus@
Coordenadoria de Acompanhamento de Egressos	egressos.sigladocampus@
Coordenadoria de Acessibilidade Educacional	naed.sigladocampus@
Departamento de Administração	dam.sigladocampus@
Coordenadoria de Gestão de Pessoas	cgp.sigladocampus@

Coordenadoria de Contratos	contratos.sigladocampus@
Coordenadoria de Compras	compras.sigladocampus@
Coordenadoria de Infraestrutura e Manutenção	infraestrutura.sigladocampus@ e/ou manutencao.sigladocampus@
Coordenadoria de Almoxarifado e Patrimônio	almoxarifado.sigladocampus@ e/ou patrimonio.sigladocampus@
Coordenadoria de Orçamento e Finanças	financeiro.sigladocampus@
Coordenadoria de Tecnologias da Informação e da Comunicação	ctic.sigladocampus@
Comissões e Grupos de Trabalho	Para Comissões e GTs sistêmicos nome_ou_sigla@ifsc.edu.br Para Comissões e GTs de um câmpus nome_ou_sigla.sigladocampus@ifsc.edu.br
Comissões de Cotas/Bancas de Heteroidentificação	Para Comissões Sistêmicas de Cotas: cotas.renda@ifsc.edu.br cotas.ppi@ifsc.edu.br cotas.pcd@ifsc.edu.br Para Comissões de um câmpus: cotas.renda.sigladocampus@ifsc.edu.br cotas.ppi.sigladocampus@ifsc.edu.br cotas.pcd.sigladocampus@ifsc.edu.br
Eleições	Para os câmpus: eleicoes.tema.sigladocampus@ifsc.edu.br ou eleicoesANO.tema.sigladocampus@ifsc.edu.br Para a Reitoria: eleicoes.tema@ifsc.edu.br ou eleicoesANO.tema@ifsc.edu.br
Representações	tipo.tema@ tipo.tema.sigladocampus@ Ex: docentes.consup@

	alunos.cepe@ alunos.agronomia.cco@ docentes.colegiado.gas@
Grêmio Estudantil e Centro Acadêmico	gremio.sigladocampus@ifsc.edu.br ca.curso-ou-sigladocurso.sigladocampus@ifsc.edu.br
Bolsistas e Estagiários	primeironome.umsobrenome@bolsista.ifsc.edu.br
Tutor	primeironome.umsobrenome@tutor.ifsc.edu.br

ANEXO III
FORMATO E DEFINIÇÕES SOBRE LISTAS E GRUPOS DE CONTAS

Finalidade	Padrão da Lista ou Grupo
Comissões	**nomecomissao**.Reitoria@ **nomecomissao**.sigla-do-campus@
Grupos de Trabalho	**nomegt.**Reitoria@ **nomegt**.sigla-do-câmpus@
Grupos de Comodatários de Celulares dos Contratos	comodatarios.celular.grupo@

Listas	Moderador(es)	Não Moderados
todos@	suporte.Reitoria@	reitor@ dircom@ dtic@
todos.docente@		
todos.tae@		