MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SERGIPE

DELIBERAÇÃO CGSIC/ IFS Nº 09, DE 03 DE ABRIL DE 2023

Aprova a Política de Controle de Acesso do Instituto Federal de Sergipe.

A PRESIDENTE DO COMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO DO INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SERGIPE, faz saber que, no uso das atribuições legais que lhe confere a Lei nº 11.892 de 29 de dezembro de 2008, em conformidade com a Portaria IFS nº 3795 de 06/12/2019, considerando a Instrução Normativa GSI nº 1 de 2/05/2020, e a decisão proferida na 2ª Reunião Ordinária do Comitê Gestor de Segurança da Informação em 2023 ocorrida em 30 de março de 2023;

RESOLVE:

CAPÍTULO I

DAS DISPOSIÇÕES PRELIMINARES

Art. 1º Esta Deliberação dispõe sobre a Política de Controle de Acesso Lógico e Físico aos recursos da rede do Instituto Federal de Educação, Ciência e Tecnologia de Sergipe – IFS, que objetiva estabelecer controles de identificação, autenticação e autorização para salvaguardar as informações do Instituto Federal de Sergipe, 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.

Art. 2º Esta Política se aplica a todas as informações, cuja o IFS seja o agente de tratamento, ao meio utilizado para este tratamento, seja digital ou físico, e as dependências físicas desta organização, 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**.**

Parágrafo Único A presente Política se aplica a todos os membros da alta administração, servidores, Funcionários Terceirizados, estagiários, Professores convidados, alunos, parceiros comerciais (consultores, agentes comerciais e convidados) que atuam em nome do IFS e fornecedores (outros contratados e subcontratados pelo IFS) e que, no âmbito dessa relação, possam acessar as áreas, equipamentos, informações, arquivos, redes e dados de titularidade ou propriedade do IFS.

Seção I

Das Definições

Art. 3 º Para os efeitos desta política considera-se:

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. AGENTES DE TRATAMENTO - o controlador ou o operador;

III. ALTA ADMINISTRAÇÃO: consiste em todo e qualquer responsável por tomar decisões de nível estratégico, independentemente da natureza da unidade gestora e das nomenclaturas utilizadas. Como membro de instância colegiada, é responsável por implementar a Política de Segurança da Informação e normas relacionadas no âmbito deste órgão;

IV. 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

V. 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);

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

VII. Comitê Gestor de Segurança da Informação (CGSIC) - instância colegiada de natureza deliberativa, de caráter permanente, instituído através da Portaria Nº 3.849/2017/IFS e convalidado pela Resolução Nº 17/2017/CS/IFS, recriado pela Portaria Nº 3795/2019/IFS, em conformidade com orientação da art. 5º, inciso VI, da IN – GSI/PR 1/2008, item 5.3.7.3 da NC – DSIC/GSI/PR 3/IN01, item 6.1.2 da ABNT NBR ISO/IEC 27002:2005; é responsável por implementar a Política de Segurança da Informação e normas relacionadas.

VIII. ETIR – Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos - 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. Anteriormente era chamada de Equipe de Tratamento de Incidentes de Rede;

IX. INCIDENTE DE SEGURANÇA - qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

X. INFORMAÇÕES SENSÍVEIS - aquelas pertinentes à origem social e étnica, à saúde, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas;

XI. INFRAESTRUTURA CRÍTICA - instalações, serviços, bens e sistemas, virtuais ou físicos, que se forem incapacitados, destruídos ou tiverem desempenho extremamente degradado, provocarão sério impacto social, econômico, político, internacional ou à segurança;

XII. LGPD - Lei Geral de Proteção de Dados Pessoais;

XIII. PERÍMETRO DE SEGURANÇA - consiste em algumas formas de barreira físicas, tecnológicas e até psicológicas para impedir invasões, inibir possíveis ações e prevenir situações de risco;

XIV. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO (POSIC) - estabelece as diretrizes gerais de segurança e controle de proteção da informação. Tais controles são descritos e padronizados pelos processos e procedimentos de segurança da informação com ferramentas e conscientizações.

XV. PROGRAMA DE GESTÃO - é uma ferramenta de gestão autorizada em ato normativo de Ministro de Estado e respaldada por norma de procedimentos gerais. Ele disciplina o exercício de atividades em que os resultados possam ser efetivamente mensurados e cuja execução possa ser realizada pelos participantes com dispensa de controle de frequência. Programa de Gestão foi regulamentado pela Resolução CS/IFS nº 107, de 10 de dezembro de 2021.

XVI. SEGURANÇA DA INFORMAÇÃO - ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

XVII. SIAPE- Sistema Integrado de Administração de Recursos Humanos;

XVIII. SIG - Sistema de Integrado de Gestão;

XIX. SISGP - Sistema do Programa de Gestão e Desempenho;

XX. SSID - Service Set Identifier ou Identificador de Conjunto de Serviços de uma rede Wi-Fi é o termo técnico para seu nome de rede.

XXI. SUSEP - Superintendência de Seguros Privados;

XXII. URL- Deuniform Resource Locator;

XXIII. USUÁRIOS DE RECURSOS DE TECNOLOGIA DA INFORMAÇÃO - servidores ocupantes de cargo efetivo ou cargo em comissão, ocupantes de emprego público em exercício, assim como funcionários de empresas prestadoras de serviços, alunos, bolsistas, estagiários e demais usuários temporários em atividade no IFS.

XXIV. VPN - *Virtual Private Network*.

CAPÍTULO II

ACESSO LÓGICO A REDE

Art. 4º O acesso lógico aos recursos da Rede Local deve ser realizado por meio de sistema de controle de acesso.

I. Terão direito a acesso lógico aos recursos da Rede Local os usuários de recursos de tecnologia da informação.

Art. 5º Para a Rede Administrativa (WIFI SSID RedeADM), o acesso local deve ser concedido e mantido pelas Coordenadorias de Tecnologia da Informação (CTI), e acesso remoto deve ser concedido e mantido pela Coordenadoria de Segurança da Informação (COSEG), baseado nas responsabilidades e tarefas de cada usuário, mediante chamado com a solicitação feita via sistema *Gestion Libre de Parc Informatique* (GLPI) ou através de outro canal de comunicação oficial disponibilizado pela Diretoria de Tecnologia da Informação (DTI), em momentos de indisponibilidade.

Parágrafo único. O acesso remoto deve ser realizado exclusivamente por *Virtual Private Network* (VPN) – Rede Virtual Privada. Para conceder a permissão para o acesso remoto, será necessário anexar ao chamado uma lista de todos osS sistemas (URL) de que precisa de acesso e comprovação que o servidor está participando do programa de gestão devidamente homologado pelo superior imediato ou apresente justificativa para o acesso remoto com a devida autorização do superior imediato caso não faça parte do programa de gestão.

Art. 6º Para a rede Acadêmica (WIFI SSID RedeLAB) os acessos dos dispositivos dos alunos, professores e demais usuários devem ser concedidos e mantidos pelas CTIs de cada campus.

Art. 7º Será disponibilizado o acesso WIFI através da rede IfsLivre para todos os alunos, colaboradores do IFS e visitantes.

I. Para os servidores técnico-administrativos, o acesso pode ser feito utilizando as credenciais da base do sistema acadêmico e terá duração de 90 dias.

II. Para professores e alunos o acesso também pode ser feito utilizando as credenciais da base do sistema acadêmico e terá duração de 90 dias.

III. Para os funcionários terceirizados e demais usuários o acesso deve ser realizado utilizando a conta de plataformas publicamente reconhecidas, como: Google ou Facebook. Para esses casos o acesso terá duração de 7 dias.

CAPÍTULO III

DO ACESSO LÓGICO AOS SISTEMAS

Art. 8° O acesso aos sistemas de uso acadêmico ou administrativo disponibilizados na web pelo IFS, será feito utilizando a credencial da base Sistema de Integrado de Gestão.

I. Essa credencial deve ser concedida ao aluno ou servidor nos primeiros dias de ingresso na instituição tendo como usuário a matrícula acadêmica no caso do aluno ou a matricula SIAPE no caso do servidor.

II. Caberá às Coordenadorias de Registro Escolar o pré-cadastro do aluno no sistema de integrado de gestão.

III. Caberá à Pró-Reitoria de Gestão de Pessoas (PROGEP) o pré-cadastro do servidor no sistema de integrado de gestão.

IV. Nos casos onde foi realizado o cadastro e o acesso não foi estabelecido caberá ao superior imediato solicitar a verificação via chamado GLPI.

CAPÍTULO IV

DA CONTA DE ACESSO LÓGICO E SENHA

Art. 9° Para utilização das estações de trabalho do IFS, será obrigatório o uso de uma única identificação (*login*) e de senha de acesso, fornecidos pela CTI, mediante solicitação formal via GLPI pelo superior imediato da unidade do requisitante.

I. Os privilégios de acesso dos usuários à Rede Local devem ser definidos pela unidade requisitante a qual o usuário está vinculado, limitando-se as atividades estritamente necessárias à realização de suas tarefas.

II. Na necessidade de utilização de perfil diferente do disponibilizado, o titular da unidade do usuário deverá encaminhar solicitação para a CTI que a examinará, podendo negá-la nos casos em que a entender desnecessária.

Art. 10 O *login* e senha são de uso pessoal e intransferível, sendo proibida a sua divulgação, sob pena de serem bloqueados pela CTI ou COSEG quando constatada qualquer irregularidade.

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

Art. 11 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, João.silva.

Parágrafo único. Nos casos da existência de conta de acesso para outro usuário, a CTI realizará outra combinação utilizando o nome completo do usuário para o qual a conta está sendo criada.

Art. 12 O padrão adotado para o formato da senha é o definido pela COSEG, que considera o tamanho mínimo de 8 caracteres, a tipologia (letras, número e símbolos) e a proibição de repetição de senhas anteriores.

I. A formação da senha da identificação (login) de acesso à Rede Local deve seguir as regras de:

a) Possuir tamanho mínimo de oito caracteres, sendo obrigatório o uso de letras e números.

b) Recomenda-se a utilização de letras maiúsculas, minúsculas e caracteres especiais ($, %, &,...);

c) 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;

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

e) Não reutilizar as últimas 05 (cinco) senhas.

II. A CTI fornecerá uma senha temporária para cada conta de acesso criada no momento da liberação dessa conta e a mesma deverá ser alterada pelo usuário quando do primeiro acesso à Rede Local.

Art. 13 As senhas de acesso serão renovadas a cada [90 (noventa)] dias, devendo o usuário ser informado antecipadamente a fim de que ele próprio efetue a mudança.

Parágrafo único. Caso não efetue a troca no prazo estabelecido, será bloqueado seu acesso à Rede Local até que a nova senha seja configurada.

CAPÍTULO V

DO BLOQUEIO E DESBLOQUEIO DA CONTA DE ACESSO

Art. 14 A conta de acesso será bloqueada nos seguintes casos:

I. Após [5 (cinco)] tentativas consecutivas de acesso errado;

II. Solicitação do superior imediato do usuário com a devida justificativa;

III. Quando da suspeita de mau uso dos serviços disponibilizados pelo IFS ou descumprimento da Política de Segurança da Informação e Comunicações – POSIC e normas correlatas em vigência.

IV. Após [100 (cem)] dias consecutivos sem movimentação pelo usuário.

Art. 15 O desbloqueio da conta de acesso à Rede Local será realizado apenas após solicitação formal do usuário ou seu superior imediato à CTI via sistema GLPI ou através de outro canal de comunicação oficial disponibilizado pela DTI, em momentos de indisponibilidade.

Art. 16 Quando do afastamento temporário do usuário, a PROGEP deve solicitar o bloqueio a CTI via sistema GLPI ou através de outro canal de comunicação oficial disponibilizado pela DTI, em momentos de indisponibilidade.

Art. 17 Quando do desligamento do usuário, a PROGEP deve solicitar o bloqueio da conta de acesso à Rede Local e da base dos sistemas integrados de gestão a CTI via sistema GLPI ou através de outro canal de comunicação oficial disponibilizado pela DTI, em momentos de indisponibilidade.

Art. 18 Quando do desligamento do Aluno, a Coordenadoria de Registro Escolar (CRE) deve solicitar o bloqueio da conta de acesso à Rede Local a CTI via sistema GLPI ou através de outro canal de comunicação oficial disponibilizado pela DTI, em momentos de indisponibilidade.

Art. 19 O acesso remoto a VPN terá validade até o último dia do ano vigente (31/12) que corresponde ao fim do programa de gestão em execução no sistema SISGP::SUSEP. Caberá ao usuário ou superior imediato fazer nova solicitação de acesso a VPN via sistema GLPI para o programa de gestão do próximo ano.

CAPÍTULO VI

DA MOVIMENTAÇÃO INTERNA

Art. 20 Quando houver mudança do usuário para outro setor, os direitos de acesso à Rede Local devem ser readequados, conforme solicitação do novo superior imediato ou da PROGEP via sistema GLPI ou através de outro canal de comunicação oficial disponibilizado pela DTI, em momentos de indisponibilidade.

Parágrafo único. As permissões de acesso devem ser imediatamente canceladas conforme solicitação do antigo superior imediato ou da PROGEP via sistema GLPI ou através de outro canal de comunicação oficial disponibilizado pela DTI, em momentos de indisponibilidade.

CAPÍTULO VII

DA CONTA DE ACESSO BIOMÉTRICO

Art. 21 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 IFS deverá tratar seus respectivos dados biométricos como dados sigilosos, preferencialmente, utilizando-se de criptografia, na forma da legislação vigente.

CAPÍTULO VIII

DOS ADMINISTRADORES

Art. 22 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.

I. Somente os técnicos das CTI's, Coordenadoria de Infraestrutura e Manutenção de Redes (COIMR) e COSEG, devidamente identificados e habilitados, terão senha com privilégio de administrador nos equipamentos locais e na rede.

II. Na necessidade de utilização de login com privilégio de administrador do equipamento local, o usuário deverá encaminhar solicitação para a CTI, que poderá negar os casos em que entender desnecessária a utilização.

III. 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 autorização formal da CTI e seguindo o catá42logo de software do IFS.

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

V. 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.

VI. Salvo para atividades específicas das CTI's, COIMR e COSEG, 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.

VII. Excepcionalmente, poderão ser concedidas identificações (login) de acesso à rede de comunicação de dados a visitante em caráter temporário após apreciação da COSEG mediante solicitação via chamado GLPI por meio das CTI's.

CAPÍTULO IX

DAS RESPONSABILIDADES

Art. 23 É de responsabilidade do superior imediato do usuário comunicar formalmente à PROGEP e a CTI o desligamento ou saída do usuário do IFS para que as permissões de acesso à Rede Local e Remoto sejam canceladas.

Art. 24 Caberá a PROGEP do IFS a comunicação imediata a CTI sobre desligamentos, férias e licenças de servidores, bolsistas e estagiários, para que seja efetuado o bloqueio momentâneo ou a revogação definitiva da permissão de acesso aos recursos.

Art. 25 É responsabilidade da Pró-Reitoria de Admininstração (PROAD) e fiscais de contrato do IFS a comunicação imediata as CTI's 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. 26 Caberá a PROEN e CRE's do IFS a comunicação imediata a CTI sobre desligamentos e licenças de alunos para que seja efetuado o bloqueio momentâneo ou a revogação definitiva da permissão de acesso aos recursos.

Art. 27 Caberá a COSEG e COIMR configurar e manter os serviços de filtragem por programas de antivírus, anti-phishing e anti-spam que poderão excluir ou bloquear automaticamente arquivos e aplicações que violem as políticas e regras configuradas na ferramenta.

Art. 28 É de responsabilidade das CTI's, COIMR, COSEG e membros da ETIR 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 e descartada qualquer hipótese de dano à infraestrutura tecnológica do IFS.

Art. 29 O usuário é 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 IFS.

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.

II. A utilização simultânea da conta de acesso à Rede Local 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.

III. O usuário não poderá, em hipótese alguma, transferir ou compartilhar com outrem sua conta de acesso e respectiva senha à Rede Local.

Art. 30 O usuário deve informar a CTI ou a ETIR através do email abuse@ifs.edu.br qualquer situação da qual tenha conhecimento que configure violação de sigilo ou que possa colocar em risco a segurança inclusive de terceiros.

Art. 31 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 completarem suas atividades ou quando se ausentarem 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;

VIII. Assinar o Termo de Responsabilidade quanto a utilização da respectiva conta de acesso.

IX. Assinar o Termo de Responsabilidade (Modelo - Anexo A) quanto a utilização da respectiva conta de acesso;

X. Em caso de necessidade de acesso remoto através da VPN, o usuário e seu superior deverão preencher e assinar o Termo de Responsabilidade (Modelo - Anexo B) informando dados necessários para este acesso.

CAPÍTULO X

DO ACESSO FÍSICO

Art. 32 Os controles de acesso físicos devem visar restringir o acesso aos equipamentos, documentos e suprimentos do IFS e à proteção dos recursos computacionais, permitindo acesso somente de pessoas autorizadas.

Art. 33 As responsabilidades pela segurança física dos sistemas e ambientes do IFS estão definidas e atribuídas a indivíduos claramente identificados.

Art. 34 O ingresso de visitantes a DTI deve ser registrado e controlado de tal forma a impedir o acesso destes às áreas de armazenamento ou processamento de informações sensíveis, salvo acompanhados e com autorização do responsável.

Art. 35 Deverão ser criados procedimentos contra incêndios e outros desastres naturais.

Art. 36 Os ativos de informação exigirão procedimentos especiais de controle de acesso físico, em conformidade com a legislação vigente.

Art. 37 Os ativos de informação deverão estar protegidos contra ações de vandalismo, sabotagem, ataques, etc, especialmente em relação àqueles ativos considerados críticos.

Art. 38 Os controles para as áreas como *datacenter* e instalações consideradas críticas deverão ser intensificados, em conformidade com a legislação vigente.

Art. 39 Deverão ser ilustrados em documentação própria, e permitido que sejam identificados, os perímetros de segurança física de cada ativo de informação por todos os que transitaram ou tiveram acesso a tais espaços, em especial às áreas e instalações consideradas críticas.

Parágrafo único. Para os fins desta Política são consideradas áreas e instalações críticas as salas cofres da DTI, racks com equipamentos, painéis de controle de energia, geradores, comunicações, cabeamentos e demais áreas com ativos de TI.

Art. 40 Todas as mídias contendo cópias de segurança (*backups*) de ativos da informação do IFS deverão, sempre que possível, estar armazenadas em perímetro de segurança.

Art. 41 Todo material, equipamento, “software” ou componente a ser retirado da DTI ou CTI’s por servidor, prestador de serviços ou pessoas autorizadas, deve seguir a norma vigente da instituição

Art. 42 Não é permitido a instalação de equipamentos na rede administrativa que não estejam homologados e autorizados pela COSEG/DTI.

Parágrafo único. Equipamentos oriundos de projeto de pesquisa, assim como de outras fontes, quando necessário e após análise da equipe da CTI local, poderão ser instalados na rede Acadêmica. Os casos omissos serão tratados por essa Diretoria.

Art. 43 Não é admitida a utilização de equipamentos gravadores de imagens, estáticas ou em movimento sem a devida autorização prévia, ressalvados os casos previstos em lei.

Art. 44 A fim de prevenir o acesso não autorizado, dano ou interferência às informações e instalações físicas do IFS, deve-se tomar as seguintes medidas:

I. Verificar a existência de falhas de segurança no perímetro ou áreas críticas que permitam o comprometimento da segurança física;

II. Proteger devidamente as portas externas contra o acesso não autorizado, com mecanismos de controle, barras, alarmes, fechaduras e etc;

III. Rever e atualizar regularmente os direitos de acesso a áreas críticas e sensíveis.

IV. Trancar e inspecionar periodicamente as áreas desocupadas;

Art. 45 Recursos tecnológicos e documentos críticos ou sensíveis devem ser mantidos em áreas seguras protegidas por um perímetro de segurança definido, com barreiras de segurança e controle de acesso. Eles devem estar fisicamente protegidos de acesso não autorizado, dano ou interferência.

Parágrafo único. Visitantes nessas áreas devem ser acompanhados e obter acesso apenas às áreas específicas, com propósitos autorizados, e esses acessos devem seguir instruções baseadas nos requisitos de segurança da área visitada. A proteção fornecida deve ser proporcional aos riscos identificados.

Art. 46 O acesso aos componentes da infraestrutura, atividade fundamental ao funcionamento dos sistemas do IFS, como painéis de controle de energia, geradores, comunicações e cabeamentos, deve ser restrito ao pessoal autorizado.

Art. 47 Nas instalações da DTI, todos os funcionários devem utilizar alguma forma visível de identificação (por exemplo: crachá), e devem informar à segurança sobre a presença de qualquer pessoa não identificada ou de qualquer estranho não acompanhado.

Art. 48 Os servidores do IFS são responsáveis por todos os atos praticados com suas identificações, tais como: crachá, carimbo, e Chaves criptográficas sob sua custódia (*tokens*).

CAPÍTULO XI

DAS CONSIDERAÇÕES FINAIS

Art. 49 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 a CTI de seu campus ou a ETIR através do email abuse@ifs.edu.br.

Art. 50 Quando houver suspeita de quebra da segurança da informação que exponha ao risco os serviços ou recursos de tecnologia, a ETIR fará a investigação, podendo interromper temporariamente o serviço afetado, sem prévia autorização.

I. Nos casos em que o ator da quebra de segurança for um usuário, a CTI comunicará os resultados ao superior imediato do mesmo para adoção de medidas cabíveis.

II. Ações que violem a POSIC ou que quebrem os controles de Segurança da Informação serão passíveis de sanções civis, penais e administrativas, conforme a legislação em vigor, que podem ser aplicadas isoladamente ou cumulativamente.

III. Processo administrativo disciplinar específico deverá ser instaurado para apurar as ações que constituem em quebra das diretrizes impostas por esta Norma e pela POSIC.

IV. A resolução de casos de violação/transgressões omissos nas legislações correlatas será resolvida pelo Comitê Gestor de Segurança da Informação - CGSIC do IFS.

Art. 51. Esta política poderá ser desdobrada em outros documentos normativos específicos, que deverão preservar coerência e alinhamento com os elementos norteadores nesta estabelecidos.

Art. 52. A política será revisada anualmente, ou ainda quando uma nova tecnologia surgir, instruções normativas existentes sofrerem alterações ou conforme necessidade do CGSIC.

Art. 53. Os casos omissos e as situações imprevistas serão encaminhados à avaliação e decisão da autoridade máxima do IFS.

Art. 54. Esta Deliberação entra em vigor em 02 de maio de 2023.

Aracaju, 03 de abril de 2023.

Ruth Sales Gama de Andrade
Presidente do CGSIC/IFS

ANEXO A

TERMO DE RESPONSABILIDADE

Pelo presente instrumento, eu _____, CPF _____, identidade _____, expedida pelo _____, em _____, e lotado no(a)_____deste Instituto. DECLARO sob pena das sanções cabíveis nos termos da _____ (legislação vigente) que assumo a responsabilidade por:

I Tratar o(s) ativo(s) de informação como patrimônio do Instituto Federal de Educação, Ciência e Tecnologia de Sergipe – IFS;

II Utilizar as informações em qualquer suporte sob minha custódia, exclusivamente, no interesse do serviço do IFS.;

III Contribuir para assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações, conforme descrito na Instrução Normativa nº 01, do Gabinete de Segurança Institucional da Presidência da República, de 27 de maio de 2020, que Dispõe sobre Estrutura de Gestão de Segurança da Informação nos órgãos e nas entidades da administração pública federal;

IV Utilizar as credenciais, as contas de acesso e os ativos de informação em conformidade com a legislação vigente e normas específicas do IFS.;

V Responder, perante o IFS., pelo uso indevido das minhas credenciais ou contas de acesso e dos ativos de informação;

VI Acessar a rede corporativa, computadores, Internet e/ou utilização de e-mail, somente com autorização (usuário/senha), por necessidade de serviço ou por determinação expressa de superior hierárquico, realizando as tarefas e operações em estrita observância aos procedimentos, normas e disposições contidas na Resolução Normativa que rege o acesso à rede corporativa, computadores, Internet e/ou utilização de e-mail;

VII Utilizar o correio eletrônico (e-mail) colocado a minha disposição somente por necessidade de serviço ou por determinação expressa de superior hierárquico, realizando as tarefas e operações, em estrita observância aos procedimentos, normas e disposições contidas na Resolução Normativa que rege o acesso à rede corporativa, computadores, Internet e/ou utilização de e-mail;

VIII Não revelar, fora do âmbito profissional, fato ou informação de qualquer natureza de que tenha conhecimento por força de minhas atribuições, salvo em decorrência de decisão competente na esfera legal ou judicial, bem como de autoridade superior;

IX Manter a necessária cautela quando da exibição de dados em tela, impressora ou na gravação em meios eletrônicos, a fim de evitar que deles venham a tomar ciência pessoas não autorizadas;

X Não me ausentar da estação de trabalho sem encerrar a sessão de uso do navegador (browser), bloquear estação de trabalho, bem como encerrar a seção do cliente de correio, garantindo assim a impossibilidade de acesso indevido por terceiros;

XI Não revelar minha senha de acesso à rede corporativa, computadores, Internet e/ou do correio eletrônico (e-mail) a ninguém e tomar o máximo de cuidado para que ela permaneça somente de meu conhecimento;

XII Responder, em todas as instâncias, pelas consequências das ações ou omissões de minha parte que possam pôr em risco ou comprometer a exclusividade de conhecimento de minha senha ou das transações a que tenha acesso.

Local, UF, _____de _____de _____.

_____

Assinatura

Nome do usuário

_____

Nome da autoridade responsável pela autorização do acesso

MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SERGIPE

ANEXO B
INSTRUÇÕES PARA PREENCHIMENTO

a) Todos os campos são de preenchimento obrigatório;

REQUERENTE/SOLICITANTE

SETOR:	
NOME:	**SIAPE:**
CARGO/FUNÇÃO:	
E-MAIL:	
INFORMAR PERÍODO DE ACESSO	
PERÍODO DE ACESSO DE: / / A / /	

DADOS DO USUÁRIO

NOME:	**SIAPE:**
CARGO/FUNÇÃO:	
E-MAIL:	**TELEFONE:**

USUÁRIO NO DOMÍNIO IFS:	

INFORMAR O IP DE REDE, URL (WWW) OU NOME DA MÁQUINA E NUM. PORTA NA REDE IFS, POIS É DE EXTREMA IMPORTÂNCIA PARA OS DEVIDOS ACESSOS.

DESTINOS: (IP, URL ou Nome da Máquina)	**PORTA:**

INFORMAR DADOS DO COMPUTADOR QUE SERÁ UTILIZADO PARA ACESSO A VPN

SISTEMA OPERACIONAL E VERSÃO	**ARQUITETURA**
	( ) **32BITs** ( ) **64BITs**

INFORMAR O ANTIVÍRUS E VERSÃO

OBSERVAÇÕES

MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SERGIPE

TERMO DE USO E RESPONSABILIDADE DE ACESSO À VPN

Este Termo de Uso e Responsabilidade de Acesso à VPN é um instrumento que vincula o Usuário cujo acesso VPN está sendo concedido após aprovação desta solicitação.

As informações constantes neste Termo comprovarão o vínculo e a validade da concessão, assim como identificarão os responsáveis de cada uma das partes e seus respectivos contatos.

A concessão de acesso somente ocorrerá mediante o preenchimento, pelo solicitante e pelo usuário, do formulário constante neste Termo. Sendo:

I Todos os campos do termo devem estar preenchidos com informações fidedignas;
II O usuário e o seu superior devem assinar em conjunto o Termo;

Não será concedido acesso completo à rede do IFS.

Não será permitida a conexão simultânea de usuários.

Não será concedido acesso se a máquina não possuir antivírus.

O cessionário deve informar imediatamente a coordenação de TI o descredenciamento ou comprometimento da senha sob sua responsabilidade.

Ao utilizar o acesso VPN, o usuário assume a responsabilidade final pelos acessos registrados por seu usuário, senha e aceita os termos de autenticidade inerentes a esses, que garantem a identidade e autenticidade de um agente e asseguram a integridade de origem.

O usuário poderá contatar a qualquer momento O IFS para esclarecer dúvidas, obter orientações e reportar situações de violação ao presente Termo e outros, através da conta de e-mail: **coseg@ifs.edu.br.**

A solicitação para criação ou renovação de usuários, senhas, para concessões em atividade, será atendida em até 5 dias úteis.

Qualquer ocorrência relevante na configuração ou disponibilidade do serviço VPN, será informada por email e/ou telefone.

Será enviado para o email informado no “Termo de Uso e Responsabilidade de Acesso à VPN”, as orientações necessárias para uso da VPN.

ARACAJU, / / /

_____	_____
COORDENADOR	USUÁRIO

ANEXO C
REFERÊNCIA LEGAL E DE BOAS PRÁTICAS

Orientação	**Secção**
Decreto 10.332/2020 - Estratégia de Governo Digital 2020-2022	Em sua íntegra
Lei Nº 13.709/2018 – Lei Geral de Proteção de Dados	CAPÍTULO VII - Seção I – Art. 46, Seção II Art. 50
Decreto Nº 9.573/2018 - Política Nacional de Segurança de Infraestruturas Críticas (PNSIC)	Anexo Art.3, Inciso I
Decreto Nº 9.637/2018 - Política Nacional de Segurança da Informação (PNSI)	CAPÍTULO I - Art.2, Incisos III e IV CAPÍTULO II - Art.3, Inciso XI CAPÍTULO VI - Seção IV – Art.15
Decreto Nº 10.222/2020 - Estratégia Nacional de Segurança Cibernética (E-CIBER)	Anexo, Item 2.3.4 e 2.3.5
Decreto Nº 10.046/2019 - Governança no Compartilhamento de Dados (GCD)	Art. 2, XXIII
Instrução Normativa 01/GSI/PR	Art.12, Inciso IV, alínea f
Acórdão 1.889/2020-TCU-Plenário	Relatório de Levantamento de Auditoria Páginas 30-32
ABNT NBR ISO/IEC 27002: 2013. Código de Prática para controles de Segurança da Informação	Itens 9 – 11.2.9 (Páginas 23 - 47)
CIS V8	CAPÍTULO 6
Guia do Framework de Segurança – LGPD	Páginas 24 - 26
Portaria GSI/PR nº 93, de 18 de outubro de 2021	Em sua íntegra