NORMA COMPLEMENTAR II
(NC-II) ACESSO FÍSICO E LÓGICO

1 OBJETIVO

Estabelecer controles de identificação, autenticação e autorização — físicos e lógicos — para assegurar que o acesso às dependências e aos sistemas de informação do Instituto Federal de Brasília (IFB) ocorra exclusivamente por meio de credenciais pessoais e intransferíveis, como crachá funcional e *login* de usuário. Esses controles visam garantir a confidencialidade, integridade, disponibilidade e autenticidade das informações institucionais, prevenindo acessos não autorizados, alterações indevidas, destruição, perda ou vazamento de dados, promovendo a segurança no acesso aos recursos tecnológicos do IFB.

2 ESCOPO

Esta norma se aplica a todas as informações tratadas pelo IFB e aos meios físicos e digitais utilizados para tal fim, abrangendo:

I. Servidores efetivos e temporários, estagiários, bolsistas, estudantes e visitantes.

II. Terceirizados, prestadores de serviço e parceiros que interagem com sistemas, redes ou espaços físicos institucionais.

III. Todos os dispositivos e ambientes da rede do IFB, inclusive os acessos remotos e físicos a data centers, laboratórios, salas técnicas, entre outros.

3 TERMOS E DEFINIÇÕES

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

II. **CONTA DE SERVIÇO:** conta de acesso à rede administrativa de computadores, necessária a um procedimento automático (aplicação, *script*, entre outros) sem qualquer intervenção humana no seu uso.

III. **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.

IV. **MFA:** sigla de autenticação de multifatores *(multifactor authentication*).

V. **CREDENCIAL DE ACESSO:** permissão concedida por autoridade competente, após o processo de credenciamento, que habilita determinada pessoa, sistema ou

organização ao acesso de recursos. A credencial pode ser física (como por exemplo um crachá), ou lógica (como por exemplo a identificação de usuário e senha).

VI. **SSO** (*Single Sign-On* ou *Login* Único): é um mecanismo de autenticação que permite a um usuário acessar múltiplos sistemas ou aplicativos utilizando apenas um conjunto de credenciais (nome de usuário e senha).

REFERÊNCIAS LEGAIS E BOAS PRÁTICAS

Orientação	Referência
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
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 Privacidade e Segurança da Informação (PPSI)	Controles 5, 6, 12 e 31
Instrução Normativa Nº 04/GSI/PR, de 26 de março de 2020	Capítulo II
Portaria GSI/PR nº 93, de 18 de outubro de 2021	Em sua íntegra

Account and Credential Management Policy Template for CIS Controls 5 and 6	Em sua íntegra
ABNT NBR ISO/IEC 27701: 2019. Técnicas de segurança — Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação — Requisitos e Diretrizes	Itens 6 – 6.6.2 (Página 16)
ISO/IEC FDIS 29151:2016(E). Information technology — Security techniques — Code of practice for personally identifiable information protection	Itens 9 – 9.2.2 e 9.2.3 (Página 11)
GSI 09/2023. OSIC (ORIENTAÇÃO DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA) — Gestão de Acesso Privilegiado (Privileged Access Management – PAM) – parte 2 de 2. Disponível em: https://www.gov.br/gsi/pt-br/ssic/osic/OSIC%2009.23	Em sua íntegra
Código de classificação de documentos e Tabela de temporalidade e destinação de documentos, relativos às atividades-meio do Poder Executivo federal *(versão 2024)*.	Item 066 e 066.32 (Página 148)

CAPÍTULO I

ACESSO LÓGICO

Art. 1º O acesso lógico aos recursos da Rede Local deve ser realizado por meio de sistema de controle de acesso. O acesso deve ser concedido e mantido pela DTIC, baseado nas responsabilidades e tarefas de cada usuário.

I - o IFB deve implementar protocolos de comunicação e redes seguros.

II - terão direito a acesso lógico aos recursos da Rede Local os usuários de recursos de tecnologia da informação.

III - para fins desta norma, consideram-se 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, estudantes, estagiários, bolsistas e demais usuários temporários em atividade no IFB.

Art. 2º O acesso remoto à rede interna da Instituição somente será permitido mediante uso de conexão segura por meio de Rede Privada Virtual (VPN), fornecida e gerenciada pela DTIC.

Art. 3º O uso da VPN é restrito a servidores ou colaboradores autorizados formalmente pela DTIC, conforme preenchimento do Termo de Responsabilidade de uso da VPN.

Art. 4º O usuário é responsável por garantir a segurança do dispositivo utilizado para acesso remoto, incluindo:

I - sistema operacional atualizado.

II - antivírus ativo e atualizado.

III - ambiente livre de softwares não autorizados ou suspeitos.

Art. 5º É vedado:

I - compartilhar credenciais de acesso à VPN com terceiros.

II - utilizar o acesso remoto para atividades pessoais ou não autorizadas.

III - manter conexões ativas sem necessidade funcional.

IV - realizar conexões simultâneas indevidas ou fora dos horários autorizados.

Art. 6º A DTIC poderá auditar, limitar ou suspender o uso da VPN a qualquer momento, caso identifique riscos, abusos ou irregularidades.

Art. 7º Infrações às normas de acesso remoto e VPN sujeitam o usuário a bloqueio do serviço e eventuais sanções administrativas, conforme a legislação aplicável e os normativos internos.

Art. 8º Deve ser utilizado o MFA (autenticação multifator) para a autenticação de acesso remoto, quando aplicável.

I - o acesso a todas as aplicações institucionais que estejam hospedadas em fornecedores deve utilizar MFA, quando aplicável.

II - o IFB deve centralizar a autenticação, autorização e auditoria (AAA) dos ativos de informação da sua infraestrutura de rede.

III - o IFB deve adotar técnicas de segmentação de rede visando limitar o acesso de forma eficiente e segura, assegurando que apenas colaboradores e dispositivos autorizados possam interagir com partes específicas da rede.

Art. 9º A DTIC, deve estabelecer e manter um inventário de todas as contas gerenciadas, este deve incluir contas de usuário, administrativas, testes e serviços. Em caso de contas de serviço, o inventário deve conter no mínimo informações de:

I - departamento proprietário.

II - data de criação/última autorização de renovação de acesso.

III - a DTIC, é responsável por validar todas as contas ativas do órgão, com base nas informações prestadas pelo setor de gestão de pessoas ou pelo setor responsável pela gestão destes usuários, sempre que houver ingresso, desligamento ou interrupção no vínculo com a instituição.

Art. 10 A DTIC deve implementar a centralização da gestão de contas por meio de serviço de diretório e/ou identidade.

Art. 11 A DTIC deve estabelecer e manter um inventário dos sistemas de autenticação e autorização da organização, tal inventário deve ser revisado periodicamente.

Art. 12 A DTIC deve centralizar o controle de acesso para todos os ativos de informação da organização por meio de um serviço de diretório ou provedor de SSO (*Single Sign-On*).

Art. 13 A DTIC deve definir e manter o controle de acesso dos usuários baseado em funções.

I - deve ser elaborada a documentação dos direitos dos acessos para cada função dentro da organização.

II - a DTIC deverá realizar análises de controle de acesso aos ativos institucionais para validar se todos os privilégios estão autorizados para a execução de atividades de cada função, este processo deve ser repetido de forma periódica ou quando novas funções e ativos de informação forem inseridos na organização.

III - ao conceder acesso a usuários que lidam com dados pessoais, deve-se limitar, estritamente, o acesso aos sistemas que processam esses dados ao mínimo necessário para cumprir os objetivos essenciais do processamento, em conformidade com o princípio da minimização de dados. Ao atribuir ou revogar os direitos de acesso concedidos deve-se incluir:

a) verificação de que o nível de acesso concedido é apropriado às políticas de acesso, além de ser consistente com outros requisitos, tais como, segregação de funções.

b) garantia de que os direitos de acesso não estão ativados antes que o procedimento de autorização esteja completo.

c) manutenção de um registro preciso e atualizado dos perfis dos usuários criados para os que tenham sido autorizados a acessar o sistema de informação e os dados pessoais neles contidos.

d) mudança dos direitos de acesso dos usuários que tenham mudado de função ou de atividades, e imediata remoção ou bloqueio dos direitos de acesso dos usuários que deixaram o IFB.

e) analisar criticamente os direitos de acesso em intervalos regulares.

Art. 14 O IFB deve implementar um processo formal de registro de usuários que tratem de dados pessoais para permitir a atribuição de direitos de acesso.

Art. 15 A DTIC deve fornecer medidas para lidar com o comprometimento do controle de acesso do usuário, como corrupção ou comprometimento de senhas ou outros dados de registro do usuário, para tanto podem ser realizadas as seguintes ações:

I - uso de um identificador de usuário único, para permitir relacionar os usuários com suas responsabilidades e ações.

II - o uso compartilhado de identificador de usuário somente será permitido para usuários de serviço, onde eles são necessários por razões operacionais ou de negócios e deverá ser aprovado e documentado.

III - a garantia de que um mesmo identificador de usuário não é emitido para outros.

Art. 16 A chefia imediata do setor a qual pertence o usuário deve ser informada formalmente, por servidores da área de TI, a respeito de qualquer evento relacionado a falhas de segurança referentes à conta do usuário e senha.

Art. 17 Qualquer anormalidade percebida pelo usuário quanto ao privilégio de seu acesso aos recursos de tecnologia da informação deve ser imediatamente comunicada à área de TI por meio de abertura de chamado na Central de Serviços.

CAPÍTULO II

SOLUÇÃO DE SEGURANÇA DE PERÍMETRO DA REDE DO IFB

Art. 18 Em conformidade com as diretrizes de segurança, a solução de segurança de perímetro da rede do IFB deve ser rigorosamente configurada para restringir e monitorar o tráfego de dados entre as redes públicas e os servidores de rede da instituição, especialmente aqueles de acesso público. Essa medida visa proteger os dados sensíveis e a infraestrutura tecnológica do IFB contra ameaças cibernéticas.

Art. 19 As regras de Solução de segurança de perímetro da rede do IFB são consideradas informações confidenciais e estratégicas, portanto, seu acesso, documentação e revisão são restritos aos responsáveis precisamente definidos pela DTIC responsáveis pela gestão da segurança da rede.

Art. 20 Em casos excepcionais, nos quais se fizer necessária a criação de regras de caráter específico, deverá ser realizada uma solicitação formal, via central de serviços, que será analisada pela DTIC e, em caso de aprovação, implementada.

CAPÍTULO III

CONTA DE ACESSO LÓGICO E SENHA

Art. 21 Para utilização das estações de trabalho e sistemas do IFB, será obrigatório o uso de uma única identificação (*login*) e de senha de acesso, fornecidos pela DTIC, mediante solicitação formal pelo titular do setor do requisitante.

I - a solicitação de acesso se encontra disponível para preenchimento na na central de serviços, disponível no SUAP.

II - as solicitações relativas à criação de cada conta devem ser mantidas registradas e armazenadas de forma segura pela DTIC.

III - a nomenclatura das contas de acesso de usuários deve seguir padrão definido pela DTIC.

IV - os privilégios de acesso dos usuários à Rede Local devem ser definidos pelo setor ao qual o usuário está vinculado, limitando-se a atividades estritamente necessárias à realização de suas tarefas.

V - na necessidade de utilização de perfil diferente do disponibilizado, a chefia imediata do setor do usuário deverá encaminhar a solicitação via central de serviços, que será examinada, podendo ser negada mediante justificativa.

Art. 22 As contas de acesso de terceirizados do IFB devem ter prazo de validade no máximo igual ao período de vigência do contrato ou período de duração de suas atividades.

Parágrafo único. Em caso de prorrogação de contrato, a conta deverá ser reativada mediante abertura de chamado.

Art. 23 O *login* e senha são de uso pessoal e intransferível, sendo proibida a sua divulgação, podendo haver bloqueios no acesso da conta.

Parágrafo único. Em caso de vazamento de senhas de contas institucionais, a ETIR (Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos) deverá comunicar imediatamente o usuário, devendo este trocar sua senha. Enquanto não houver a troca da senha, o usuário terá o seu acesso bloqueado.

Art. 24 Todas as contas de acesso criadas deverão ser vinculadas a uma pessoa física. É vedada a criação de usuários genéricos para acesso à rede. Essa medida visa

a segurança da rede, a rastreabilidade e identificação do indivíduo caso ocorra um incidente de segurança.

Parágrafo único. Em casos excepcionais, onde houver a necessidade temporária da criação de um usuário padrão para atender um público específico (por exemplo, em eventos institucionais) para o uso de recursos computacionais, será necessária a sua devida formalização e autorização da DTIC, devendo este usuário ser removido posteriormente.

Art. 25 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.

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

Art. 26 O padrão adotado para o formato da senha é o definido pela DTIC que considerará o tamanho mínimo de 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:

a) possui tamanho mínimo de 10 (dez) caracteres, sendo recomendado o uso de letras e números.

b) recomenda-se o uso de MFA, quando possível.

c) utilização de letras maiúsculas, minúsculas e caracteres especiais ($, %, &,@, …).

d) 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.

e) não utilizar termos óbvios, tais como: Brasil, IFB, senha, usuário, *password* ou *system*.

f) não reutilizar as últimas três senhas.

g) recomenda-se evitar a constituição de senha com os seguintes padrões:

1. nome ou parte do nome de usuário.

2. identificador do usuário (ID), mesmo que os caracteres estejam embaralhados.

3. nome de membros de sua família ou de amigos íntimos.

4. nome de pessoas ou lugares em geral.

5. nome do Sistema Operacional ou da máquina que está sendo utilizada.

6. nomes próprios.

7. datas.

8. números de telefone, carteira de identidade ou de outros documentos pessoais.

9. placas ou marcas de automóveis.

10. palavras que constam de dicionários em qualquer idioma.

11. letras ou números repetidos.

12. letras seguidas do teclado do computador (ASDFG, YUIOP).

13. a senha não poderá conter parte do nome do usuário, por exemplo: caso o usuário tenha o nome Jose da Silva, sua senha não deve conter partes do nome como "1221jose" ou "1212silv".

II - a DTIC 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. 27 As senhas de acesso serão renovadas a cada 180 (cento e oitenta) 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, poderá ser bloqueado o acesso até que a nova senha seja configurada.

Art. 28 Todos os usuários devem:

I - manter a confidencialidade das senhas.

II - não compartilhar senhas.

III - não anotar senhas em papel ou em qualquer lugar que possam ser acessadas por terceiros.

IV - alterar a senha sempre que existir qualquer indicação de possível comprometimento do sistema ou da própria senha.

Art. 29 Todos os critérios definidos acima poderão ser auditados pela DTIC.

Art. 30 A base de dados de senhas deve ser armazenada com criptografia.

CAPÍTULO IV

BLOQUEIO, DESBLOQUEIO, DESATIVAÇÃO E EXCLUSÃO DA CONTA DE ACESSO

Art. 31 A conta de acesso poderá ser 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 IFB ou descumprimento da Política de Segurança da Informação e Comunicação – PoSIC e normas correlatas em vigência.

IV - após 180 (cento e oitenta) dias consecutivos sem movimentação pelo usuário, salvo em situações específicas.

V - em caso de vazamento de senhas.

VI - em casos de investigação devidamente instruídos pela corregedoria do IFB, ou por determinação judicial.

Art. 32 A conta de acesso deverá ser desativada, a partir de solicitação formal pelo setor responsável nos seguintes casos:

I - falecimento.

II - aposentadoria.

III - exoneração.

IV - encerramento de contrato.

V - outros afastamentos que caracterizem encerramento do vínculo com a instituição.

Art. 33 Transcorridos cinco anos do término do vínculo institucional com o IFB, as contas de usuários bloqueadas poderão ser excluídas, conforme item 066.32 da Tabela de Temporalidade e Destinação de Documentos Relativos às Atividades-Meio do Poder Executivo Federal.

Art. 34 As contas de usuários estudantes que possuírem vínculo institucional findado com o IFB terão sua conta removida após um período de seis meses contados a partir da data de encerramento do vínculo.

Art. 35 O desbloqueio da conta de acesso poderá ser realizado após a solicitação formal do usuário ou da chefia imediata do usuário a DTIC, a depender do caso.

Art. 36 A DTIC deve, de forma periódica, realizar a remoção, identificação ou a desabilitação de usuários genéricos ou com identificação duplicada, salvo em situações devidamente justificadas.

Art. 37 A DTIC deve configurar o bloqueio automático de sessão nos ativos após um período de inatividade preestabelecido. Tal prazo pode ser específico para cada tipo de ativo.

Art. 38 A DTIC deve, sempre que possível, priorizar a revogação/desativação de contas com o objetivo de manter dados e logs para possíveis auditorias.

CAPÍTULO V

ACESSO FÍSICO

Art. 39 O IFB deve definir perímetros de segurança para proteger ambientes e ativos contra acesso físico não autorizado, danos e interferências de acordo com as diretrizes a seguir:

I - definir a localização e resistência dos perímetros de acordo com os requisitos de segurança da informação relacionados aos ativos que se encontram dentro dos perímetros.

II - proteger os ambientes seguros contra acessos não autorizados por meio de mecanismos de controle de acesso, como fechaduras tradicionais ou digitais, que possibilitem autenticação por biometria, senhas, PINS ou cartões de acesso.

a) o IFB deve executar testes nos mecanismos de controle de acesso em períodos pré-definidos para assegurar a funcionalidade total do equipamento.

b) os mecanismos de controle de acesso devem ser monitorados pelo setor responsável.

III - estabelecer uma área de recepção ou outros meios de controle de acesso físico a ambientes que não for conveniente a implementação de mecanismos de controle de acesso.

Art. 40 O acesso físico a ambientes seguros ou ativos de tratamento e armazenamento de dados do IFB é destinado apenas a pessoal autorizado.

Art. 41 O IFB deve manter um processo de gestão de acessos para fornecimento, revisão periódica, atualização e revogação das autorizações.

Art. 42 O IFB deve implementar e manter seguro logs ou registro físico de todos os acessos aos ativos de informação.

Art. 43 O acesso a ambientes seguros ou ativos de tratamento e armazenamento de dados por fornecedores ou prestadores de serviços será concedido somente quando necessário e de acordo com as seguintes diretrizes:

I - para fins específicos e autorizados.

II - autorização concedida pelo setor responsável.

III - supervisionado e monitorado.

Art. 44 Os ativos de armazenamento e tratamento de dados que se encontrem fora do IFB devem ser protegidos contra perda, roubos, danos e acesso físico não autorizados conforme as seguintes diretrizes:

I - não deixar o ativo sem vigilância em locais públicos e inseguros.

II - proteger o ativo contra riscos associados a visualização de informações por outra pessoa.

III - implementar as funcionalidades de rastreamento e limpeza remota.

Art. 45 O IFB deve estabelecer uma política ou normativo equivalente sobre a gestão de ativos de informação, de acordo com as seguintes diretrizes:

I - exigir autorização para a saída de ativos de informação do IFB.

II - armazenar ativos de informação em local seguro de acordo com a classificação de suas informações.

III - criptografar os dados de ativos de informação de acordo com a classificação de suas informações.

IV - manter cópias de segurança de dados dos ativos de informação de acordo com a classificação de suas informações.

Art. 46 O IFB deve elaborar uma política ou normativo equivalente que defina condições e restrições pertinentes ao acesso físico nos dispositivos de trabalho remoto, levando em consideração as seguintes diretrizes:

I - segurança física do local de trabalho remoto.

II - regras e orientações quanto ao acesso de familiares e visitantes ao dispositivo.

Art. 47 Quando houver mudança do usuário para outro setor ou o usuário ocupar uma nova função, os direitos aos perfis de acesso referentes ao setor anterior devem ser revogados, mediante solicitação formal do setor de origem.

CAPÍTULO VI

CONTA DE ACESSO BIOMÉTRICO

Art. 48 A conta de acesso biométrico, quando implementada em ambientes onde houver guarda de ativos de informação e de rede, tais como salas técnicas, datacenters, 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 IFB deverá tratar seus respectivos dados biométricos como dados sigilosos, preferencialmente, utilizando-se de criptografia, na forma da legislação vigente.

CAPÍTULO VII

ADMINISTRADORES

Art. 49 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 servidores do setor de TI de cada unidade, devidamente identificados e habilitados por sua chefia imediata, 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 DTIC, 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 do TI.

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.

VI - salvo para atividades específicas do setor de TI, não será concedida a identificação (*login*) para acesso administrativo a dispositivos e servidores de rede.

VII - a DTIC deve implementar o MFA para todas as contas de administrador, quando houver possibilidade.

VIII - o usuário com privilégio de administrador não deve realizar atividades gerais de computação, como navegação na Internet, *e-mail* e uso do pacote de

produtividade. Estas atividades deverão ser realizadas preferencialmente a partir da conta primária não privilegiada do usuário.

IX - ao tratar dados pessoais o IFB deve observar o princípio do privilégio mínimo como regra, para garantir que o usuário receba apenas os direitos mínimos necessários para executar suas atividades, para tanto podem ser realizadas as seguintes ações:

a) remover os direitos de administrador nos dispositivos finais.

b) remover todos os direitos de acesso root e admin aos servidores de rede (equipamentos) e utilizar tecnologias que permitam a elevação granular de privilégios conforme a necessidade, ao mesmo tempo em que fornecem recursos claros de auditoria e monitoramento.

c) eliminar privilégios permanentes (privilégios que estão “sempre ativos”) sempre que possível.

d) limitar a associação de uma conta privilegiada ao menor número possível de pessoas.

e) minimizar o número de direitos para cada conta privilegiada.

CAPÍTULO VIII

RESPONSABILIDADES

Art. 50 É de responsabilidade da chefia imediata do usuário comunicar formalmente à ao setor de gestão de pessoas e à DTIC o desligamento ou saída do usuário do IFB para que as permissões de acesso à Rede Local sejam canceladas.

Art. 51 É responsabilidade da PRAD a comunicação imediata ao Setor responsável pela gestão dos acessos 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. 52 É de responsabilidade da DTIC 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 IFB.

Parágrafo Único. Os serviços serão filtrados por programas de antivírus, *anti-phishing* e *anti-spam* e, caso violem alguma regra de conformidade ou configuração, serão bloqueados ou excluídos automaticamente.

Art. 53 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 IFB.

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. 54 O usuário deve informar a ETIR qualquer situação da qual tenha conhecimento que configure violação de sigilo ou que possa colocar em risco a segurança inclusive de terceiros.

Art. 55 É dever de o 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 (Modelo – Anexo I) quanto a utilização da respectiva conta de acesso.

CAPÍTULO IX

DISPOSIÇÕES GERAIS

Art. 56 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 ETIR.

Art. 57 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 ETIR comunicará os resultados à autoridade máxima da unidade responsável por esse usuário, 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 omissas nas legislações correlatas será resolvida pelo CGD do IFB.

Art. 58 As dúvidas e os casos omissos na aplicação desta Norma Complementar serão dirimidos pelo Comitê Gestor de Segurança da Informação ou, em sua ausência, pelo Comitê de Governança Digital.

Art. 59 Esta norma complementar entra em vigor na data de sua publicação.

Quadro de Revisão

Revisão	Descrição
Fev-Jul/2025	Atualização de termos e conceitos, ajustes e contextualização de textos de acordo com o cenário institucional atual.
Ago-Set/2025	Contribuições dos Campi - Técnicos de TI e Diretores-Gerais.

Abr/2026	Aprovação pelo CGD.

Elaborador por:	**GT - Atualização das Normas Complementares da PoSIC** Aysilon Melo da Silva Bruno Nepomuceno de Oliveira Daniel Pereira de Sousa Emannuel Travassos Brito Hugo Silva Faria João Bezerra da Silva Júnior João Victor de Araujo Oliveira Luciana Bastos Matos Paulo Henrique Borges Silva Sérgio Dias Saldanha Waldene Aparecida Silva Watanabe

Aprovado por	Ato autorizativo
Comitê de Governança Digital - CGD	Súmula 1/2026 - DTIC/IFBRASILIA, de 23 de abril de 2026

ANEXO I

INSTITUTO FEDERAL DE BRASÍLIA - IFB

TERMO DE RESPONSABILIDADE

Pelo presente instrumento, eu _____, CPF _____, identidade _____, expedida pelo _____, em _____, 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 IFB;

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

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 IFB;

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

VI. Acessar a rede administrativa ou acadêmica, 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 sessão 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 e seu setor organizacional

_____
Nome da autoridade responsável pela autorização do acesso