RESOLUÇÃO Nº 122, DE 29 MAIO DE 2024 – CONSUNI/UFT

Estabelece a Política de Controle de Acesso Lógico com as diretrizes de orientação, monitoramento e avaliação no âmbito da Universidade Federal do Tocantins (UFT).

O Egrégio Conselho Universitário (Consuni) da Universidade Federal do Tocantins (UFT), reunido em sessão ordinária realizada no dia 29 de maio de 2024, no uso de suas atribuições legais e estatutárias, e

CONSIDERANDO, que os riscos decorrentes de falhas na gestão da segurança da informação são de toda ordem e podem representar desde problemas relacionados à integridade de dados públicos e pessoais, passando pelo vazamento de informações sigilosas, confidenciais e pessoais, bem como podendo provocar impactos econômicos negativos em caso de indisponibilidade de serviços ou falhas em sistemas e bases de dados;

CONSIDERANDO, o Decreto nº 10.332/2020, que institui a Estratégia de Governo Digital 2020-2022;

CONSIDERANDO, a Lei nº 12.527/2011 - Lei de Acesso à Informação (LAI);

CONSIDERANDO, o art. 46 da Lei Geral de Proteção de Dados, Lei nº 13.709/2018, de 14 de agosto de 2018, que prevê que "Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito";

CONSIDERANDO, o Decreto nº 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação (PNSI), que dispõe sobre a governança da segurança da informação, no âmbito da administração pública federal, com a finalidade de assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação em âmbito nacional;

CONSIDERANDO, os incisos I, II e III do Decreto nº 9.573/2018, que aprovou a Política Nacional de Segurança de Infraestruturas Críticas (PNSIC);

CONSIDERANDO, os itens 2.3.4 e 2.3.5 do Decreto nº 10.222/2020 - Estratégia Nacional de Segurança Cibernética (E-CIBER) que tratam da elevação dos níveis de proteção das infraestruturas críticas;

CONSIDERANDO, o inciso XXIII, art 2º do Decreto nº 10.046/2019, que trata da Governança no Compartilhamento de Dados (GCD), em especial, das ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

CONSIDERANDO, o item 12.3 da Norma ABNT NBR ISO/IEC 27001:2013, Código de Prática para controles de Segurança da Informação, itens 9 - 11.2.9 (páginas 23 - 47);

CONSIDERANDO, o Guia do Framework de Privacidade e Segurança da Informação (PPSI), controles 5 e 6;

CONSIDERANDO, a Portaria GSI/PR nº 93, de 18 de outubro de 2021, Glossário de Segurança da Informação;

CONSIDERANDO, a *Account and Credential Management Policy Template for CIS Controls 5 and 6;*

CONSIDERANDO, o Capítulo IV da Instrução Normativa nº 03/GSI/PR, de 28 de maio de 2021, que trata da Gestão da Continuidade de Negócios em Segurança da Informação;

RESOLVE:

Art. 1° Aprovar a Política de Controle de Acesso Lógico com as diretrizes de orientação, monitoramento e avaliação no âmbito da Universidade Federal do Tocantins (UFT), conforme anexo desta Resolução.

Art. 2° A Política de Controle de Acesso Lógico (PCAL) da Universidade Federal do Tocantins (UFT) observará os princípios, objetivos e diretrizes estabelecidos nesta Política, bem como às disposições constitucionais, legais e regimentais vigentes.

Art. 3° Esta Resolução entra em vigor na data de sua publicação, conforme dados do processo nº 23101.002839/2023-44.

LUIS EDUARDO BOVOLATO:51368498191

Assinado digitalmente por LUIS EDUARDO BOVOLATO:51368498191
ND: C=BR, O=ICP-Brasil, OU=videoconferencia, OU=33683111000107, OU=Secretaria da Receita Federal do Brasil - RFB, OU=ARSERPRO, OU=RFB e-CPF A3, CN=LUIS EDUARDO BOVOLATO:51368498191
Razão: Eu sou o autor deste documento
Localização:
Foxit PDF Reader Versão: 2023.2.0

LUÍS EDUARDO BOVOLATO
Reitor

EMC.

UNIVERSIDADE FEDERAL DO **TOCANTINS**

POLÍTICA DE CONTROLE DE ACESSO LÓGICO COM AS DIRETRIZES DE ORIENTAÇÃO, MONITORAMENTO E AVALIAÇÃO NO ÂMBITO DA UNIVERSIDADE FEDERAL DO TOCANTINS (UFT).

Anexo da Resolução n° 122/2024 - Consuni
Aprovada pelo Conselho Universitário em 29 de maio de 2024.

Versão 2.0
Palmas/TO, 2024

POLÍTICA DE DE CONTROLE DE ACESSO LÓGICO COM AS DIRETRIZES DE ORIENTAÇÃO, MONITORAMENTO E AVALIAÇÃO NO ÂMBITO DA UNIVERSIDADE FEDERAL DO TOCANTINS (UFT).

COMITÊ DE GOVERNANÇA DIGITAL (CGD)

Luís Eduardo Bovolato
Reitor

Marcelo Leineker Costa
Vice-Reitor

Eduardo José Cezari
Pró-Reitor de Graduação

Maria Santana Ferreira dos Santos Milhomem
Pró-Reitora de Extensão

Rafhael Sanzio Pimenta
Pró-Reitor de Pesquisa e Pós-Graduação

Kherlley Caxias Batista Barbosa
Pró-Reitor de Assistência Estudantil

Eduardo Andrea Lemus Erasmo
Pró-Reitor de Avaliação e Planejamento

Ary Henrique Morais de Oliveira
Pró-Reitor de Tecnologia da Informação e Comunicação

Michelle Matilde Semiguen Lima Trombini Duarte
Pró-Reitora de Gestão e Desenvolvimento de Pessoas

Carlos Alberto Moreira de Araújo Júnior
Pró-Reitor de Administração e Finanças

COMITÊ GESTOR DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO (CGTIC)

Ary Henrique Morais de Oliveira

Pró-Reitor de Tecnologia da Informação e Comunicação

Olivia Tozzi Bittencourt
Diretora de Infraestrutura Tecnológica

Glauco Batista Sousa
Coordenador de Segurança da Informação

Werley Teixeira Reinaldo
Diretor de Soluções Digitais

Anna Paula de Sousa Parente Rodrigues
Coordenadora de Soluções para a Educação

Samuel Barbosa Costa da Silva
Coordenador de Soluções para a Gestão

Aislan Max Gomes Coelho
Analista em Tecnologia da Informação

Jefferson Victor Araújo
Analista em Tecnologia da Informação

Juliano Alves Rios
Analista em Tecnologia da Informação

Junior Fernandes de Oliveira
Técnico em Tecnologia da Informação

Luis Ferreira de Oliveira Junior
Técnico em Tecnologia da Informação

Marluzio Da Silva Leite
Analista em Tecnologia da Informação

Controle de versões:

1.0	13/02/2023	Coordenação de Segurança da Informação	Versão Inicial do Documento
1.1	29/05/2024	Coordenação de Segurança da Informação	Correção do documento
1.2	07/02/2024	Comitê de Segurança da Informação	Análise e correção do documento
1.3	09/02/2024	Diretoria de Soluções Digitais (DSD)	Análise e correção do documento
1.4	21/02/2024	Pró-Reitoria de Gestão de Pessoas (PROGEDEP)	Análise e correção do documento
2.0	21/02/2024	Coordenação de Segurança da Informação	Correção do documento
2.0	26/02/2024	Comitê de Governança Digital	Aprovação no CGD

2.0	28/05/2024	Comissão de Legislação e Normas	Aprovação na CLN/CONSUNI
2.0	29/05/2024	Conselho Universitário	Aprovação no Consuni

Contatos:

Glauco Batista de Sousa	(63) 3229-4032	internet@uft.edu.br
Ediane Dias dos Santos	(63) 3229-4032	protic@uft.edu.br

TERMOS E DEFINIÇÕES

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.

CONTROLE DE ACESSO LÓGICO - conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso ao uso de recursos computacionais. Via de regra, requer procedimentos de autenticação.

MFA - Múltiplo Fator de Autenticação, a autenticação *multifator* é um método de autenticação eletrônica no qual um usuário recebe acesso a um site, aplicativo ou sistema somente após apresentar com sucesso duas ou mais evidências a um mecanismo de autenticação: conhecimento, posse e inerência.

SETOR RESPONSÁVEL PELA GESTÃO DE ACESSOS – setor máximo responsável pela Tecnologia da Informação da reitoria da UFT ou designado por ela.

SETOR RESPONSÁVEL PELA GESTÃO DE PESSOAS – setor máximo responsável pela Gestão de Pessoas da UFT ou designado por ela.

SETOR RESPONSÁVEL PELA GESTÃO DE MÃO-DE-OBRA TERCEIRIZADA - Setor(es) responsável(is) pela(s) contratação(ões) ou acordo(s) institucional(is) da(s) aplicação(ões) ou serviço(s) disponibilizado(s) na UFT.

SSO - *Single sign-on*, solução de autenticação que permite que os usuários efetuem login com um único ID em qualquer um dos vários sistemas de software relacionados, mas independentes. O *single sign-on* permite que o usuário efetue login uma vez e acesse os serviços sem reinserir os fatores de autenticação.

VPN - Rede Virtual Privada, cria uma conexão de rede privada entre dispositivos através da Internet. As VPNs são usadas para transmitir dados de forma segura em redes públicas.

REDE DE DADOS DA UFT - Ambiente virtual da UFT composto por serviços de comunicação, sistemas, sites e aplicativos.

USUÁRIOS DE RECURSOS DE TECNOLOGIA DA INFORMAÇÃO: Pessoas naturais que acessam os serviços, equipamentos e sistemas da UFT.

CAPÍTULO I
PROPÓSITO

Art. 1º A PCAL estabelece controles de identificação, autenticação e autorização para salvaguardar as informações da UFT com o objetivo 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 Considera-se que as credenciais: logins de acesso dos sistemas de informações e demais métodos de autenticação secundários (*tokens*, cartões, biométricos), são pessoais e intransferíveis e são o único método legítimo pelo qual o direito de acesso lógico podem ser exercidos.

Art. 3º Os controles de autorização, identificação e autenticação garantem que apenas usuários autorizados tenham acesso lógico e façam uso dos sistemas de informação da UFT.

ESCOPO

Art. 4º Esta Política se aplica a todas as informações, cuja a UFT seja o agente de tratamento, onde o meio utilizado para este tratamento seja digital, bem como a qualquer pessoa que interaja exercendo controle administrativo, técnico ou operacional, mesmo que eventual, desses meios de tratamento. Especificamente, inclui:

I. todos os funcionários, sejam servidores efetivos ou temporários, da UFT;

II. todos os contratados e terceiros que trabalham para a UFT;

III. todas as pessoas naturais que sejam parceiros ou seus representantes e que acessam a rede e os sistemas de informação da UFT.

CAPÍTULO II
ACESSO LÓGICO

Art. 5º O acesso lógico aos recursos da Rede de Dados da UFT deve ser realizado por meio de sistema de controle de acesso. O acesso deve ser concedido e mantido pelo Setor responsável pela gestão de acessos, baseado nas responsabilidades e tarefas de cada usuário.

I. terão direito a acesso lógico aos recursos da Rede de Dados da UFT os usuários de recursos de tecnologia da informação;

II. para fins desta Resolução, consideram-se usuários de recursos de tecnologia da informação servidores ocupantes de cargo efetivo ou cargo em comissão, ocupantes de emprego público em exercício, alunos e egressos, assim como funcionários de empresas prestadoras de serviços, estagiários e demais usuários temporários em atividade na UFT;

III. o acesso remoto deve ser realizado por meio de Rede Virtual Privada

(VPN), após as devidas autorizações;

IV. deve ser utilizado o Múltiplo Fator de Autenticação (MFA) para a autenticação de acesso remoto;

V. o acesso a todas as aplicações corporativas ou de terceiros que estejam hospedados em fornecedores deve utilizar MFA.

Art. 6º O Setor responsável pela gestão de acessos, 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.

Art. 7º O Setor responsável pela gestão de acessos, é responsável por validar todas as contas ativas do órgão, a cada 180 (cento e oitenta), dias.

Art. 8º O Setor responsável pela gestão de acessos deve implementar a centralização da gestão de contas por meio de serviço de diretório e/ou identidade.

Art. 9º O Setor responsável pela gestão de acessos deve estabelecer e manter um inventário dos sistemas de autenticação e autorização da organização, tal inventário deve ser revisado periodicamente.

Art. 10. O Setor responsável pela gestão de acessos 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.

Art. 11. O Setor responsável pela gestão de acessos deve definir e manter o controle de acesso dos usuários baseado em funções.

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

II. o Setor responsável pela gestão de acessos 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.

CAPÍTULO III
CONTA DE ACESSO LÓGICO E SENHA

Art. 12. Para utilização das estações de trabalho da UFT, será obrigatório o uso de uma única identificação (login) e de senha de acesso, fornecidos pelo Setor responsável pela gestão de acessos, mediante solicitação formal pelo titular da unidade do

requisitante – quando necessário, com as devidas informações:

I. o formulário de solicitação de acesso se encontra disponível para preenchimento na Intranet da UFT ou via formulário específico no SEI;

II. os privilégios de acesso dos usuários à Rede de Dados da UFT devem ser definidos pela unidade requisitante ao qual o usuário está vinculado, limitando-se a atividades estritamente necessárias à realização de suas tarefas;

III. na necessidade de utilização de perfil diferente do disponibilizado, o titular da unidade do usuário deverá encaminhar solicitação para a Setor responsável pela gestão de acessos que a examinará, podendo negá-la nos casos em que a entender desnecessária.

Art. 13. O login e senha são de uso pessoal e intransferível, sendo proibida a sua divulgação, sob pena de serem bloqueados pelo Setor 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. 14. 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: glauco.barbosa.

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

Art. 15. O padrão adotado para o formato da senha é o definido pelo Setor responsável pela gestão de acessos, que considera 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 de:

a. possuir tamanho mínimo de oito caracteres, sendo obrigatório o uso de letras e números, para contas que utilizam MFA e 14 caracteres para contas que não utilizam MFA;

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 03 (três) senhas.

II. o Setor responsável pela gestão de acessos 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 de Dados da UFT.

Art. 16. 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, será bloqueado seu acesso à Rede de Dados da UFT até que a nova senha seja configurada.

CAPÍTULO IV
BLOQUEIO, DESBLOQUEIO E CANCELAMENTO DA CONTA DE ACESSO

Art. 17. 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 pela UFT ou descumprimento da Política de Segurança da Informação e normas correlatas em vigência;

IV. Após 60 (sessenta) dias consecutivos sem movimentação pelo usuário.

Art. 18. O desbloqueio da conta de acesso à Rede de Dados da UFT será realizado apenas após solicitação formal do superior imediato do Setor responsável pela gestão de acessos ou em sistema específico, alterando a senha vigente, do usuário.

Art. 19. Quando do afastamento temporário do usuário, a conta de acesso deve ser bloqueada a pedido do superior imediato ou do Setor responsável pela Gestão de Pessoas ou por iniciativa do próprio usuário.

Art. 20. A conta de acesso não utilizada há mais de 180 (cento e oitenta) dias poderá ser suspensa, sendo que a deleção do acesso aos dados de todos os sistemas a ela vinculada, poderá ocorrer em 180 dias após a suspensão.

Art. 21. O Setor responsável pela gestão de acessos, 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 - vide Política de Gestão de Ativos de TI.

Art. 22. O Setor responsável pela gestão de acessos deve, sempre que possível, priorizar a revogação/desativação de contas com o objetivo de manter dados e logs para possíveis auditorias.

CAPÍTULO V

MOVIMENTAÇÃO INTERNA

Art. 23 Quando houver mudança do usuário para outro setor, os direitos de acesso à Rede de Dados da UFT devem ser readequados, conforme solicitação do novo superior imediato ou do Setor responsável pela Gestão de Pessoas.

I. o novo superior imediato ou o Setor responsável pela Gestão de Pessoas deve realizar a solicitação de novos acessos de acordo com novo setor/função do usuário;

II. os direitos de acesso antigos devem ser imediatamente cancelados, conforme solicitação do antigo superior imediato ou do Setor responsável pela Gestão de Pessoas.

CAPÍTULO VI
CONTA DE ACESSO BIOMÉTRICO

Art. 24. A conta de acesso biométrico, quando implementada, poderá 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. A UFT deverá tratar seus respectivos dados biométricos como dados sigilosos, preferencialmente, utilizando-se de criptografia, na forma da legislação vigente.

CAPÍTULO VII
ADMINISTRADORES

Art. 25. 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 de TI devidamente habilitados pelo Setor responsável pela gestão de acessos, devidamente identificados, 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 Setor responsável pela gestão de acessos, 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 Setor responsável pela gestão de acessos;

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 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;

VII. o acesso à rede de comunicação de dados a visitantes se dará exclusivamente por meio de login na rede UFT-Visitantes com login por meio do usuário GOV.BR;

VIII. o setor responsável pela gestão de acessos deve implementar o MFA para todas as contas de administrador;

IX. o Setor responsável pela gestão de acessos deve restringir os privilégios de administrador a contas de administrador dedicados nos ativos de informação, para que o usuário com privilégio de administrador não consiga 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.

CAPÍTULO VIII
RESPONSABILIDADES

Art. 26. É de responsabilidade do superior imediato do usuário comunicar formalmente ao Setor responsável pela Gestão de Pessoas o desligamento ou saída do usuário da UFT, para que as permissões de acesso à Rede de Dados da UFT sejam revogadas.

Art. 27. Caberá ao Setor responsável pela Gestão de Pessoas da UFT a comunicação imediata ao Setor responsável pela gestão de acessos sobre desligamentos, férias e licenças de servidores e estagiários, para que seja efetuado o bloqueio momentâneo ou a revogação definitiva da permissão de acesso aos recursos.

Art. 28. Fica a cargo do setor/servidor responsável pela gestão da atividade que originou a entrada do colaborador externo, a instrução processual de comunicação ao setor de Gestão de Pessoas da Unidade a entrada do novo colaborador. Afim de prover o cadastro inicial e conceder acesso ao perfil base.

Art. 29. É de responsabilidade do Setor responsável pela gestão de acessos 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 da UFT.

I. os serviços serão filtrados por programas de antivírus, *anti-phishing* e *anti-spam* e, caso viole alguma regra de configuração, serão bloqueados ou excluídos

automaticamente;

II. nenhum técnico da UFT terá acesso ao conteúdo das informações armazenadas nos equipamentos servidores da UFT.

Art. 30. O usuário é responsável por todos os acessos realizados através de sua conta de acesso e por possíveis danos causados à Rede de Dados da UFT e a recursos de tecnologia custodiados ou de propriedade da UFT.

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 de Dados da UFT 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 de Dados da UFT.

Art. 31. O usuário deve informar ao Setor responsável pela gestão de acessos qualquer situação da qual tenha conhecimento que configure violação de sigilo ou que possa colocar em risco a segurança inclusive de terceiros.

Art. 32. 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 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;

VIII. aceitar o Termo de Responsabilidade (Modelo - Anexo A) quanto a utilização da respectiva conta de acesso.

CAPÍTULO IX
DISPOSIÇÕES FINAIS

Art. 33. 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 ao Setor responsável pela gestão de acessos.

Art. 34. Quando houver suspeita de quebra da segurança da informação que exponha ao risco os serviços ou recursos de tecnologia, a Setor responsável pela gestão de acessos 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, o Setor responsável pela gestão de acessos comunicará os resultados ao superior imediato do mesmo para adoção de medidas cabíveis;

II. ações que violem a Política de Segurança da Informação 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 Política de Segurança da Informação;

IV. a resolução de casos de violação/transgressões omissas nas legislações correlatas será resolvida pelo Comitê de Segurança da Informação da UFT.

Art. 35. Esta Resolução entra em vigor na data de sua publicação, conforme dados do processo nº 23101.002839/2023-44.

ANEXO A – Modelo de Termo de Responsabilidade

SERVIÇO PÚBLICO FEDERAL
UNIVERSIDADE FEDERAL DO TOCANTINS - UFT

TERMO DE RESPONSABILIDADE

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

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

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 da UFT;

V. Responder, perante a UFT, 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 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.