UNIVERSIDADE FEDERAL DO AMAZONAS
UFAM

Política de controle de acesso à informação e aos recursos e serviços de tecnologia da informação e comunicação

Outubro
2024

POLÍTICA DE CONTROLE DE ACESSO À INFORMAÇÃO E AOS RECURSOS E SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

UNIVERSIDADE FEDERAL DO AMAZONAS

Professor Doutor Sylvio Mário Puga Ferreira

Reitor

COMITÊ DE GOVERNANÇA DIGITAL

Professor Doutor Sylvio Mário Puga Ferreira

Reitor

David Lopes Neto

Pró-Reitor de Ensino de Graduação

Adriana Malheiro Alle Marie

Pró-Reitor de Pesquisa e Pós-Graduação

Almir Oliveira de Menezes

Pró-Reitor de Extensão

Maria Vanusa do Socorro de Souza Firmo

Pró-Reitor de Gestão de Pessoas

Maria da Glória Vitório Guimarães

Pró-Reitor de Planejamento e Desenvolvimento Institucional

Ângela Neves Bulbol de Lima

Pró-Reitor de Administração e Finanças

Jorge Carlos Magno Silva de Lima

Diretor do Centro de Tecnologia da Informação e Comunicação

Nycolle Oliveira Souza Santos

Encarregada pelo Tratamento de Dados Pessoais

Carlos Moisés Medeiros

Ouvidor

Dinorvan Fanhaimpork

Auditor

CENTRO DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

Jorge Carlos Magno Silva de Lima

Diretor

COORDENAÇÃO DE SEGURANÇA DA INFORMAÇÃO

Márcia Regina Moraes de Paula

Coordenadora de Segurança da Informação

PRÓ-REITORIA DE ENSINO DE GRADUAÇÃO

David Lopes Neto

PRÓ-REITORIA DE PESQUISA E PÓS-GRADUAÇÃO

Adriana Malheiro Alle Marie

PRÓ-REITORIA DE GESTÃO DE PESSOAS

Maria Vanusa do Socorro de Souza Firmo

EQUIPE TÉCNICA DE ELABORAÇÃO E REVISÃO

Gilberto Aires Libania

Márcia Regina Moraes de Paula

Lendel do Santos Monteiro

Pedro da Rocha Figueiredo

Robert Pessinga da Silva

Histórico de Versões

Data	Versão	Descrição	Autor
02/06/2022	1.0	Elaboração da Política de Controle de Acesso à Informação e aos Recursos e Serviços de Tecnologia da Informação e Comunicação.	Equipe Técnica de Elaboração e Revisão
25/07/2023	1.1	Revisão na Coordenação de Segurança da Informação e Comunicação.	Equipe Técnica de Elaboração e Revisão
09/10/2023	1.2	Revisão nas Coordenações do CTIC.	Equipe Técnica de Elaboração e Revisão
27/05/2024	1.3	Revisão e atualização em conformidade aos Controles 5.1, 5.2, 5.3, 5.4, 5.5, 5.6, 6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 31.3, 31.4 e 31.6 do PPSI.	Equipe Técnica de Elaboração e Revisão
16/09/2024	1.4	Revisão e atualização em conformidade aos Controles 12.3, 12.5, 12.6, e 12.7 do PPSI.	Equipe Técnica de Elaboração e Revisão
10/10/2024	1.5	Revisada, atualizada e aprovada por membros do CGD.	Equipe Técnica de Elaboração e Revisão, e CGD.

SUMÁRIO

1. Disposições preliminares

1.1. Da finalidade e objetivo

Esta instrução normativa tem por finalidade regulamentar o uso e o acesso aos Recursos de Tecnologia da Informação e Comunicação da UFAM, e integra a Política de Segurança da Informação e Comunicação da UFAM e suas fundamentações legais e normativas, como também deve estar alinhada com uma gestão de continuidade de negócio institucional, disciplinando o acesso à rede de dados institucional, o uso da Internet, o uso dos sistemas institucionais e o uso dos demais recursos de TIC, visando a garantia dos serviços à comunidade acadêmica de acordo com boas práticas de utilização. O uso e a administração dos recursos de TIC devem estar relacionados ao ensino, pesquisa, extensão, administração e, em conformidade com a missão e princípios da UFAM.

1.2. Fundamentações legais e normativas

As referências legais e normativas utilizadas para a elaboração desta política são:

a) Decreto nº 10.332, 28 de abril de 2020 - Estratégia de Governo Digital 2020-2022, em sua íntegra;
b) Lei nº 13.709, de 14 de agosto de 2018: institui a Lei Geral de Proteção de Dados Pessoais (LGPD). Art. 6º, inciso VII, Art. 46, Art. 47, Art. 49, Art. 50;
c) Decreto nº 9.573/2018 - Política Nacional de Segurança de Infraestruturas Críticas (PNSIC), anexo, Art. 3, Inciso I;
d) Decreto nº 9.637/2018 - Política Nacional de Segurança da Informação (PNSI), Cap. I, Art.2, Incisos III e IV, Cap. II, Art.3, Inciso XI, Cap. VI, Seção IV, Art. 15;
e) Decreto nº 10.222/2020 - Estratégia Nacional de Segurança Cibernética (E-CIBER), Anexo, Item 2.3.4 e 2.3.5;
f) Decreto nº 10.046/2019 - Governança no Compartilhamento de Dados (GCD), Art. 2, XXIII;
g) Decreto nº 7.845, DE 14 DE NOVEMBRO DE 2012, Regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento;

h) Lei 12.965, de 23 de abril de 2014 - Estabelece princípios, garantias, direitos e deveres para uso da internet no Brasil - Marco Civil da Internet;
i) Instrução Normativa nº 1/GSI/PR, de 27 de maio de 2020: Dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal, Art.12, Inciso IV, alínea f;
j) Instrução Normativa nº 2 /GSI/PR, de 5 de fevereiro de 2013: Dispõe sobre o Credenciamento de segurança para o tratamento de informação classificada, em qualquer grau de sigilo, no âmbito do Poder Executivo Federal;
k) Instrução Normativa nº 4 /GSI/PR, de 26 de março de 2020: Dispõe sobre os requisitos mínimos de Segurança Cibernética que devem ser adotados no estabelecimento das redes 5G;
l) Instrução Normativa nº 5 /GSI/PR, de 30 de agosto de 2021: Dispõe sobre os requisitos mínimos de segurança da informação para utilização de soluções de computação em nuvem pelos órgãos e pelas entidades da administração pública federal;
m) Instrução Normativa nº 6 /GSI/PR, de 23 de dezembro de 2021: Estabelece diretrizes de segurança da informação para o uso seguro de mídias sociais nos órgãos e nas entidades da administração pública federal.
n) Norma Complementar nº 01 /IN02/NSC/GSI/PR, e seus anexos (A e B); Disciplina o Credenciamento de Segurança de Pessoas Naturais, Órgãos e Entidades Públicas e Privadas para o Tratamento de Informações Classificadas. (Publicada no DOU nº 123, de 28 de junho de 2013-Seção 1);
o) Norma Complementar nº 07 /IN01/DSIC/GSI/PR, Estabelece as Diretrizes para Implementação de Controles de Acesso Relativos à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta;
p) Norma Complementar nº 09 /IN01/DSIC/GSI/PR, Estabelece orientações específicas para o uso de recursos criptográficos em Segurança da Informação e Comunicações, nos órgãos ou entidades da Administração Pública Federal (APF), direta e indireta. (Publicada no DOU nº 134, de 16 Jul 2014-Seção 1);
q) Norma Complementar nº 12/IN02/NSC/GSI/PR, de 27 de Junho de 2013: Disciplina o credenciamento de segurança de pessoas naturais, órgãos e entidades públicas e privadas para o tratamento de informações classificadas;

r) Norma ABNT NBR ISO/IEC 27001:2022: especifica requisitos para estabelecer, implementar, manter e melhorar continuamente um Sistema de Gestão de Segurança da Informação (SGSI);

s) Norma ABNT NBR ISO/IEC 27002:2022: fornece diretrizes para práticas de gestão de segurança da informação e código de prática para controles de Segurança da Informação, itens 9-11.2.9 (pág. 23 - 47);

t) Norma ABNT NBR ISO/IEC 27014:2021; Segurança da informação, segurança cibernética e proteção da privacidade - Governança da segurança da informação;

u) Norma ABNT NBR ISO/IEC 27701:2019; Técnicas de segurança - Extensão das normas ABNT NBR ISO/IEC 27001 e 27002 para gestão da privacidade da informação - Requisitos e Diretrizes, itens 6-6.6.2 (Página 16);

v) Norma 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);

w) Política de Segurança da Informação e Comunicação da Universidade Federal do Amazonas: Art. 10, item i. - Conscientização e Treinamento: tem por objetivo internalizar conceitos e boas práticas de segurança da informação na cultura da instituição, por meio de ações permanentes de divulgação, treinamento e educação, para minimizar riscos de segurança da informação;

x) Modelo de Política de Gestão de Controle de Acesso do Programa de Privacidade e Segurança da Informação (PPSI) do Governo Federal: tem por finalidade prover diretrizes para a gestão de controle de acesso e gestão de contas e segurança aplicada a privacidade;

y) Guia do Framework de Privacidade e Segurança da Informação, estabelece que os controles 5, 6, 12 e 31, tem por finalidade prover diretrizes para gestão de contas e gestão do controle de acesso e segurança aplicada à privacidade institucional, (pág. 42-44, 69-70) e gestão da infraestrutura de redes;

z) Framework de controles CIS (Center for Internet Security) Versão 8, controles 5 e 6, (pág. 21-26);

aa) Portaria GSI/PR nº 93, de 18 de outubro de 2021, em sua íntegra;

bb) 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;

1.3. Das definições

Para os efeitos desta política, consideram-se:

a) 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;

b) Áreas e instalações de acesso restrito: áreas e instalações que contenham documento com Informação Classificada, ou que, por sua utilização ou finalidade, demandarem proteção, as quais têm seu acesso restrito às pessoas autorizadas pelo órgão ou entidade;

c) 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;

d) AAA: sigla de autenticação, autorização e auditoria;

e) Autenticação: processo que busca verificar a identidade digital de uma entidade de um sistema, no momento em que ela requisita acesso a esse sistema. O processo é realizado por meio de regras preestabelecidas, geralmente pela comparação das credenciais apresentadas pela entidade com outras já pré-definidas no sistema, reconhecendo como verdadeiras ou legítimas as partes envolvidas em um processo;

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

g) Auditoria: processo de exame cuidadoso e sistemático das atividades desenvolvidas, cujo objetivo é averiguar se elas estão de acordo com as disposições planejadas e estabelecidas previamente, se foram

implementadas com eficácia e se estão adequadas e em conformidade à consecução dos objetivos;

h) Autenticação de dois fatores ou duplo fator de autenticação (2 factor authentication, 2FA): processo de segurança que exige que os usuários forneçam dois meios de identificação antes de acessarem suas contas;

i) 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);

j) Computação em nuvem: modelo de fornecimento e entrega de tecnologia de informação que permite acesso conveniente e sob demanda a um conjunto de recursos computacionais configuráveis, sendo que tais recursos podem ser provisionados e liberados com mínimo gerenciamento ou interação com o provedor do serviço de nuvem (PSN);

k) Confidencialidade: propriedade pela qual se assegura que a informação não esteja disponível ou não seja revelada à pessoa, ao sistema, ao órgão ou à entidade não autorizados nem credenciados;

l) Conta de serviço: conta de acesso à rede corporativa de computadores, necessária a um procedimento automático (aplicação, script, entre outros) sem qualquer intervenção humana no seu uso;

m) 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;

n) CGD: Comitê de Governança Digital, instância interna responsável por determinar as políticas de segurança da informação;

o) CTIC: Centro de Tecnologia da Informação e Comunicação, setor técnico responsável pela gestão de TI na instituição;

p) CSIRT (Computer Security Incident Response Team): sigla internacional para designar um grupo de resposta a incidentes de segurança, responsável por tratar incidentes de segurança para um público alvo específico;

q) OSIC: Orientação de Segurança da Informação e Cibernética;
r) PAM: Gestão de Acesso Privilegiado, traduzindo (Privileged Access Management)
s) 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);
t) Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR): grupo de agentes públicos com a responsabilidade de prestar serviços relacionados à segurança cibernética para o órgão ou a entidade da administração pública federal, em observância à política de segurança da informação e aos processos de gestão de riscos de segurança da informação do órgão ou da entidade.
u) Single Sign On (SSO): solução tecnológica que permite que diversos aplicativos com senhas de acesso diferentes possam ser acessados de forma transparente e segura pela utilização de uma única senha principal ou meio de identificação pessoal (como a biometria ou um personal identification number- PIN, por exemplo);
v) Setor responsável pela gestão de acessos: setor responsável pelo vínculo do usuário com a instituição. É o setor responsável pelo controle de acesso do usuário, ou seja, por autorizar o acesso do usuário aos recursos ou desautorizar em casos como o de afastamento temporário ou definitivo.
w) VPN: sigla de rede privada virtual traduzindo (virtual private network).

1.4. Do escopo

As normas e diretrizes apresentadas nesta política se aplicam aos agentes públicos da UFAM, aos estudantes vinculados ou qualquer pessoa, física ou jurídica, que acesse os recursos computacionais cuja a UFAM seja o agente de tratamento, independente do meio utilizado para este tratamento. Esta política contempla o controle de acesso lógico à informação e aos recursos computacionais e também abrange o controle de acesso físico das áreas e instalações de acesso restrito definidas nesta política, bem como qualquer pessoa que circule nas dependências ou que interaja exercendo controle administrativo, técnico ou operacional, mesmo que eventual, desses meios de tratamento, sejam

servidores efetivos ou temporários, prestadores de serviços contratados ou terceirizados, funcionários de parceiros que acessam fisicamente as dependências ou que acessam a rede e sistemas de informação.

1.5. Vedações

Fica vedado o uso dos recursos de TIC na UFAM para:

a) Armazenar, trocar, processar conteúdo inapropriado, ofensivo, obsceno, pornográfico, sexualmente sugestivo, abusivo, discriminatório, difamatório, ameaçador, de ódio, preconceituoso, que infrinja as leis de propriedade intelectual ou as leis de privacidade.
b) Divulgar informações sigilosas ou confidenciais, pessoais ou sensíveis sem a devida autorização;
c) Realizar importunação virtual (cyberbullying) ou assédio e discriminação de qualquer espécie, ou qualquer forma de violência verbal ou escrita contra membros da comunidade universitária ou qualquer outra pessoa;
d) Atividades ilegais, como acesso não autorizado a sistemas, distribuição de conteúdo ilegal, fraude eletrônica, entre outros fins não relacionados às atividades acadêmicas, tais como atividades comerciais, jogos eletrônicos não autorizados, entretenimento não educativo, etc.;
e) Promover apologia à violência de qualquer tipo;
f) Escanear tráfego de rede, buscar vulnerabilidades, explorar vulnerabilidades em qualquer recurso de TIC, exceto quando realizado pela ETIR no desempenho de suas atividades;
g) Obter benefícios e/ou ganhos pessoais, propaganda e promoção de interesses particulares;
h) Utilizar-se dos recursos computacionais para assuntos pessoais, ao qual só é permitido em caráter estritamente restrito, de forma a não comprometer as atividades e os interesses da instituição;

1.6. Responsabilidades

Compete ao gestor das unidades constituintes da UFAM fazer cumprir as normas contidas nesta política.

É de responsabilidade do superior imediato do usuário comunicar formalmente à Setor responsável pela Gestão de Pessoas e o Setor responsável pela gestão dos acessos

o desligamento ou saída do usuário da UFAM, para que as permissões de acesso à sejam revogadas.

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

É de responsabilidade do CTIC 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 ou dispositivo que esteja realizando atividade que coloque em risco a segurança da rede, até que seja verificada a situação, é descartada qualquer hipótese de dano à infraestrutura tecnológica da UFAM.

Compete aos usuários a responsabilidade por todos os acessos realizados através de sua conta de acesso e por possíveis danos causados aos recursos de tecnologia custodiados ou de propriedade da UFAM.

São responsabilidades dos usuários dos recursos de TIC:

a) Manter a integridade e utilização de sua estação de trabalho, protegendo as telas de seus dispositivos no caso de sua ausência temporária do local do equipamento, devendo bloqueá-lo ou desconectar-se para coibir acessos indevidos.
b) Manter suas credenciais de acesso sempre em sigilo, não devendo ser anotadas em meios físicos ou eletrônicos de forma insegura, e não poderá, em hipótese alguma, transferir ou compartilhar com outrem sua conta de acesso e respectiva senha;
c) Alterar sua senha de acesso periodicamente ou sempre que suspeitar que ela foi comprometida;
d) Evitar a utilização simultânea da conta de acesso em mais de uma estação de trabalho ou notebook, não compartilhando suas credenciais com terceiros, sendo responsabilidade do titular da conta de acesso os riscos que a utilização paralela implica;
e) Utilizar os recursos de forma adequada, seguindo as políticas e diretrizes estabelecidas pela instituição para fins acadêmicos e administrativos,

respeitando as leis, regulamentos e as boas práticas de segurança da informação;

f) Cumprir a legislação aplicável, incluindo as leis de proteção de dados, direitos autorais, privacidade e segurança da informação;
g) Adotar uma conduta ética, evitando a disseminação de conteúdo ofensivo, discriminatório, difamatório ou ilegal. Devendo respeitar os direitos e a privacidade de outros usuários; e
h) Notificar imediatamente setores competentes ou a ETIR, qualquer situação que tenha conhecimento que configure um incidente de segurança da informação ou violação de dados sigilosos ou que possa colocar em risco a segurança inclusive de terceiros, para que as medidas adequadas possam ser tomadas para mitigar os danos.

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

a) Não permitir a interferência externa caracterizada como invasão, monitoramento ou utilização de sistemas por terceiros, e outras formas;
b) Evitar sobrecarga de redes, de dispositivos de armazenamento de dados ou de outros, para não gerar indisponibilidade de informações internas e externas;
c) Interromper a conexão aos sistemas e adotar medidas que bloqueiem o acesso de terceiros, sempre que completarem suas atividades ou quando ausentar-se do local de trabalho por qualquer motivo;
d) 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;
e) Não divulgar a terceiros ou a outros usuários dispositivos ou programas de segurança existentes em seus equipamentos ou sistemas;
f) Utilizar corretamente os equipamentos de informática e conservá-los conforme os cuidados e medidas preventivas estabelecidas;
g) Não divulgar suas senhas, mesmo que temporárias, e nem permitir que terceiros tomem conhecimento delas, reconhecendo-as como pessoais e intransferíveis;
h) Assinar eletronicamente o Termo de Responsabilidade (ANEXO A) quando da concessão/renovação da respectiva credencial de conta de acesso e aos ativos de informação em conformidade com a legislação vigente e normas específicas da Universidade Federal do Amazonas.

2. Gestão do controle de acesso lógico

O acesso lógico aos recursos tecnológicos oferecidos deverá ser realizado pelos setores responsáveis pela gestão do controle de acessos, utilizando sistema de concessão/revogação do controle de acesso ou através de ofício encaminhado ao CTIC, sendo este apenas mantenedor dos recursos de TIC.

O CTIC deve centralizar a autenticação, autorização e auditoria (AAA) dos ativos de informação através do gerenciamento de sua infraestrutura de redes, e implementar protocolos de comunicação e de redes seguros, e que o acesso a todas as aplicações corporativas ou de terceiros que estejam hospedados em fornecedores deve utilizar MFA, e também 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.

O setor responsável pela gestão do controle de acessos é a unidade responsável pelo vínculo do usuário com a instituição e compete a estes setores a execução de ações e providências para atribuição ou revogação de acesso aos recursos de TIC de acordo com o estado de vinculação de cada usuário com a instituição, incluindo vínculos temporários que devem ser avaliados pelos setores competentes. Desta forma, a credencial de acesso deve ser concedida e mantida por estes setores, baseado nas responsabilidades e funções de cada usuário obedecendo os níveis de privilégios de acesso e de acordo com as definições abaixo elencadas na tabela A abaixo:

Usuário	**Responsável pela gestão do controle de acesso**
Discentes de graduação	PROEG
Discentes de pós-graduação	PROPESP
Técnicos administrativos	PROGESP
Docentes	PROGESP
Estagiários/Bolsistas internos e externos	Unidade responsável pelo vínculo
Terceirizados/Temporários	Unidade responsável pelo vínculo

Tabela A

Para fins desta política, 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 terceirizados ou de empresas

prestadoras de serviços, estagiários/bolsistas internos e externos, alunos e demais usuários com vínculo institucional.

O Setor responsável pela gestão dos 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:

a. Departamento/unidade/setor proprietário.
b. Tipo de conta e nível de privilégio de acesso.
c. Data de criação/última autorização de renovação de acesso;
d. Data de validade ou tempo de contrato para concessão de acesso em caso de funcionários terceirizados/temporários ou de empresas prestadoras de serviços, estagiários/bolsistas internos e externos, para programação de revogação do acesso.
e. Validação de todas as contas ativas do órgão, a cada 90 (noventa) dias, será de responsável pelo departamento/unidade/setor de gestão dos acessos.

Deve-se estabelecer e manter um inventário dos sistemas de autenticação e autorização da organização, tal inventário deve ser revisado periodicamente.

O Setor responsável pela gestão dos acessos deve centralizar o controle de acesso para todos os ativos de informação da organização por meio de um serviço de diretório e/ou identidade ou provedor de SSO combinado com MFA.

O Setor responsável pela gestão dos acessos 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. O Setor responsável pela gestão dos 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.

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 a instituição;
e. Analisar criticamente os direitos de acesso em intervalos regulares.

O Setor responsável pela gestão dos acessos deve implementar um processo formal de registro de usuários que tratem de dados pessoais para permitir atribuição de direitos de acesso e 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. O 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, onde eles são necessários por razões operacionais ou de negócios e deverá ser aprovado e documentado;
III. A garantia de que a identificação única de usuários e a autenticação de suas credenciais (como senhas, tokens, certificados digitais ou biometria), não seja emitido para outros.

Para utilização das estações de trabalho no âmbito do campus/campis UFAM, será obrigatório o uso de uma única identificação (login) e de senha de acesso, fornecidos pelo Setor responsável pela gestão dos acessos, mediante solicitação formal pelo titular da unidade do requisitante ao CTIC.

I. A solicitação de acesso deve ser feita através de Sistemas GLPI que se encontra disponível no site suportectic.ufam.edu.br.
II. Os privilégios de acesso dos usuários à Rede Local ou Sistemas 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 o CTIC que a examinará, podendo negá-la nos casos em que a entender desnecessária.

2.1. Criação de conta de acesso lógico

As contas de cada perfil de usuário deverão ser administradas e autorizadas por meio do portal institucional e-Campus ou sistemas internos, pelos respectivos gestores de acesso lógico de acordo com a tabela A.

O usuário dos recursos de TIC deverá através do sistema escolher um nome de usuário e assinar digitalmente o Termo de Responsabilidade, conforme modelo anexo B desta política.

Serão utilizados para acesso aos recursos de TIC credencial de acesso. A credencial será composta de número de CPF ou nome de usuário e respectiva senha de acesso.

2.1.1. Formação de nomes de usuário

As contas de acesso quanto ao seu padrão de formação para nomes de usuário (login) seguirão as regras da norma “Padrão de Formação de Endereços de Correio Eletrônico Caixas Postais Individuais” do Governo Federal (ANEXO B desta política).

Casos não previstos na norma deverão ser excepcionalmente encaminhados ao CGD.

2.1.2. Formação de senhas

O padrão adotado para o formato da senha é o definido pelo (modelo anexo B desta política) que considera o tamanho mínimo de caracteres, a tipologia (letras, número e símbolos) e a proibição de repetição de senhas anteriores. A formação da senha deve seguir os seguintes critérios sempre que possível:

a) Possuir tamanho mínimo de oito caracteres, sendo obrigatório o uso de letras, números e/ou caracteres especiais para contas que utilizam MFA e 14 caracteres para contas que não utilizam MFA;

b) Utilizar letras maiusculas, 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: senha, usuário, password ou system, etc.

e) Não reutilizar as últimas 03 (três) senhas.

2.1.3. Autenticação multifator

Fica estabelecido a adoção mínima de duplo fator de autenticação (2FA) obrigatório para os sistemas compatíveis com a implementação da autenticação multifatorial (MFA), medida que adiciona duas ou mais camadas extras de proteção contra acessos indevidos ou não autorizados a dados pessoais ou sistemas.

O uso do MFA deve ser obrigatório para técnicos, docentes, terceirizados e estagiários/bolsistas, sendo facultado aos discentes. Como também deve ser utilizado o MFA para a autenticação de acesso remoto e acesso a todas as aplicações institucionais ou de terceiros que estejam hospedados em fornecedores ou parceiros. Será implementado um MFA robusto de alta resistência para todas as contas de acesso privilegiado de administrador combinadas com SSO.

2.1.4. Registro de acessos

Fica estabelecida a obrigatoriedade de armazenamento dos registros associados aos recursos de TIC de todos os acessos, incidentes e eventos cibernéticos, incluindo informação sobre sessões e transações, por período determinados pela legislação vigente seguindo as normas da Política de Logs e Auditoria da UFAM. Desta forma, mesmo após o cancelamento do acesso lógico aos recursos, o período vigente sob leis e normas devem ser observados.

2.2. Bloqueio e desbloqueio de conta de acesso

A conta de acesso será bloqueada nos seguintes casos:

- Após 5 (cinco) tentativas consecutivas de acesso errado;
- Após 180 (cento e oitenta) dias consecutivos sem movimentação pelo usuário.
- Por solicitação do superior imediato do usuário com a devida justificativa formal encaminhada ao setor responsável pela gestão de acessos;

- Por parte do CTIC quando da suspeita de mau uso dos recursos tecnológicos disponibilizados ou descumprimento da Política de Segurança da Informação - PoSIC e normas correlatas em vigência.
- Quando do afastamento temporário do usuário, a conta de acesso deve ser bloqueada pelo setor responsável pela gestão de acessos.
- Em recursos de TIC específicos, tais como e-mail, compartilhamento de arquivos, etc, utilizados além dos limites de cota estabelecidos, até a readequação por parte do usuário à cota estipulada.
- O Setor responsável pela Tecnologia da Informação, deve configurar o bloqueio automático de sessão nos ativos após um período de inatividade preestabelecido, e tal prazo pode ser específico para cada tipo de ativo.

O desbloqueio da conta de acesso será realizado apenas após solicitação formal do superior imediato do usuário ao setor responsável pela gestão de acessos no caso de docentes e técnicos, ou diretamente ao setor responsável pela gestão de acessos no caso de discentes.

Caso seja avaliado reiterado mau uso dos serviços, a conta será permanentemente bloqueada devendo o transgressor recorrer ao CGD para encaminhamento da situação.

2.3. Revogação de Acesso

O cancelamento do acesso lógico aos recursos de TIC deverá ser realizado pelo setor responsável pela gestão de acessos associado ao usuário quando da ocasião da perda de vínculo do usuário com a instituição.

Quando houver mudança do usuário para outro setor ou o usuário ocupar uma nova função, conforme solicitação do antigo superior imediato os direitos de acesso aos recursos devem ser imediatamente revogados e o novo superior imediato ou setor responsável pela gestão de acesso deve realizar a solicitação de novos acessos de acordo com novo setor/função do usuário.

O Setor responsável pela gestão dos acessos, deve garantir a implementação de um processo formal de cancelamento de usuários que administrem ou operem sistemas e serviços que tratem de dados pessoais. Tal processo deverá incluir:

I. A imediata remoção ou desabilitação de usuário que tenha deixado a instituição;

II. A remoção e identificação, de forma periódica, ou a desabilitação de usuários com os mesmos identificadores.

O Setor responsável pela Tecnologia da Informação deve, sempre que possível, priorizar a revogação/desativação de contas com o objetivo de manter dados e logs para possíveis auditorias.

2.4. Contas de acesso privilegiado (administrador)

O uso de contas de acesso privilegiado é de uso restrito aos técnicos do CTIC, com a concessão de permissão compatível com a natureza da função técnica e execução da tarefa desempenhada.

O CTIC deve implementar um MFA robusto de alta resistência para todas as contas de acesso privilegiado de administrador combinadas com SSO.

O CTIC será responsável pelo gerenciamento de acesso privilegiado (PAM), como estratégia para proteger os sistemas e contas mais importantes da instituição contra acesso não autorizado. Como medidas fundamentais de boas práticas de PAM, serão realizadas as seguintes ações:

a. Implementar o Acesso de Menor Privilégio: Reduzindo a superfície de ataque limitando o acesso de contas privilegiadas apenas ao que é necessário, garantindo que os usuários tenham acesso apenas às informações e sistemas essenciais para suas funções.
b. Monitorar a Atividade de Contas Privilegiadas: Identificar e inventariar todas as contas privilegiadas na rede e gerenciar adequadamente, verificando quem está acessando essas contas e como elas estão sendo utilizadas.
c. Restringir o Uso de Contas Privilegiadas: Usuários das contas de acesso privilegiado de uso restrito, devem ter contas de usuário padrão para uso cotidiano, fazendo login nas contas privilegiadas apenas ao realizar atividades privilegiadas.

O CTIC 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.

d. Validação Explícita e Privilégios Mínimos: basear-se em princípios de confiança zero, validação explícita e pressuposição de violação.

Ao tratar dados pessoais o Setor responsável pela gestão dos acessos 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 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.

Na necessidade de utilização de login com privilégio de administrador por terceiros para acesso a rede ou sistemas, devem ser definidos e solicitados pela unidade requisitante ao qual o usuário está vinculado, limitando-se a atividades estritamente necessárias à realização de suas tarefas, encaminhando solicitação formal para o CTIC, que avaliará os riscos envolvidos, podendo negar nos casos em que entender pela não aceitação dos riscos.

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

Em caso de estação de trabalho, se concedida a permissão ao usuário como administrador local, esse será responsável por manter a integridade da máquina, não podendo instalar, desinstalar ou remover qualquer programa em desacordo com esta e as demais políticas de segurança. Caso constatada a irregularidade, o usuário perderá o acesso como administrador, não mais podendo requerer outra permissão.

Salvo para atividades específicas da área responsável pela gestão da tecnologia da informação, 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.

2.5. Conta de acesso biométrico

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 (MFA) devendo a instituição tratar seus respectivos dados biométricos como dados sigilosos, preferencialmente, utilizando-se de criptografia, na forma da legislação vigente.

2.6. Contas de acesso temporário

Excepcionalmente, poderão ser concedidas credenciais de acesso aos recursos de TIC a visitante em caráter temporário.

O responsável pelo vínculo temporário institucional do visitante deverá encaminhar antecipadamente solicitação formal ao CGD que avaliará a viabilidade da concessão, podendo este negar nos casos em que entender que não há viabilidade de negócio ou técnica a respeito da concessão.

3. Uso adequado do acesso

Essencial para garantir a segurança da informação e privacidade o controle de acesso objetiva estabelecer controles de identificação, autenticação e autorização para salvaguardar as informações no âmbito da Universidade Federal do Amazonas, em qualquer meio, seja digital ou físico, a fim de evitar a quebra da segurança da informação e acessos não autorizados que impliquem em risco potencial ou que os sistemas de informação possam ser acessados ilicitamente e sejam comprometidos.

Considera-se, portanto, que a conta de acesso aos recursos de TIC é de uso pessoal e intransferível, sendo vedado o seu compartilhamento em qualquer hipótese e que as credenciais: crachá de identificação funcional e login de acesso aos sistemas de informações, e o único método legítimo exercido que dá o direito de acesso físico e/ou lógico.

As responsabilidades do usuário incluem, principalmente, os cuidados para a manutenção da segurança dos recursos, tais como sigilo da senha e o monitoramento de suas ações, evitando sua utilização indevida. O usuário que não estiver utilizando a informação, não deverá deixar exposto na tela, reduzindo assim o risco de acesso não autorizado, perda e danos à informação.

As contas de acesso devem ser utilizadas somente para fins designados nesta política e para os quais estiverem devidamente autorizados.

É dever dos usuários reportar imediatamente ao superior imediato e ao CTIC os casos de violação de credenciais de acesso, acidental ou não, sua ou de terceiros.

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 CTIC ou ETIR.

Acessar Conta de Usuário(a) pertencente a outra pessoa, qualquer que seja o motivo do uso.

4. Uso adequado dos serviços

Os recursos e serviços de TIC devem ser utilizados em conformidade com os usos e restrições assim definidos:

a) Correio eletrônico: para comunicações de caráter estritamente acadêmico e administrativo, sendo vedado o uso como repositório de arquivos e uso pessoal.
b) Edoc: repositório de documentos administrativos. Utilizado para armazenar, divulgar e oferecer acesso aos documentos produzidos para os portais institucionais.
c) Google Drive: repositório de arquivos de trabalho. Vedado o uso para publicação de documentos oficiais.
d) Google Workspace: serviços disponíveis para uso estritamente acadêmico e administrativo, devendo ser observadas também a Política de Uso aceitável ("AUP") quanto ao uso.
e) Rede de dados: para uso estritamente acadêmico e administrativo, devendo ser observadas também as políticas de segurança da Rede Nacional de Pesquisa (RNP) quanto ao uso da Internet.
f) Telefonia Digital: para comunicações de caráter estritamente administrativo, sendo vedado o uso particular.
g) Microsoft Online Services: serviços disponíveis para uso estritamente acadêmico e administrativo, devendo ser observadas também a Política de Uso aceitável ("AUP") quanto ao uso.

5. Controle de acesso remoto

O CTIC deve garantir que usuários através de dispositivos remotos utilizem uma rede virtual privada (VPN) e se conectem em uma infraestrutura centralizada de autenticação, autorização e auditoria (AAA) dos ativos em rede segura, gerenciados pela

instituição antes de acessar os dispositivos e recursos, utilizando protocolos de comunicação e mecanismos de gestão de redes seguros, como a utilização obrigatória do MFA combinadas com SSO, para a autenticação de acesso remoto visando garantir o acesso seguro, além de recomendar o uso da proteção de antivírus, firewall do S.O., bloqueadores de browsers, etc.

As informações acessadas, processadas ou armazenadas em locais de trabalho remoto (teletrabalho) devem ser protegidas. As atividades de trabalho remoto devem estar em conformidade com as políticas de segurança da informação.

Nos casos de trabalho remoto deve-se observar a classificação da informação que pode ser tratada e os sistemas internos e serviços que o usuário do trabalho remoto está autorizado a acessar expressamente por sua chefia imediata.

6. Controle de acesso em redes sociais

O perfil de contas institucionais em redes sociais deve ser gerido pela Assessoria de Comunicação (ASCOM), sendo obrigatória a publicidade nos portais institucionais, de forma a possibilitar que o público em geral possa reconhecer sem equívocos quais perfis são tidos como oficiais e portanto, unicamente confiáveis, e tratando como falsos outros que porventura existam nessas redes sociais.

Sempre que a plataforma de rede social disponibilizar mecanismo de verificação de conta, os responsáveis devem solicitar o selo de verificação visando evidenciar para o público que trata-se de perfil autêntico.

Para os demais perfis institucionais em redes sociais, ficam os chefes das unidades administrativas ou acadêmicas responsáveis por garantir que o perfil, quando criado, esteja publicizado no portal institucional associado e que o selo de verificação do perfil seja providenciado junto à plataforma de rede social utilizada.

Cada parte acima citada fica responsável pelo controle de acesso à conta de acesso ao perfil em rede social, devendo estes adotarem as orientações contidas nesta política para mitigação dos riscos associados a uso indevido e acesso não autorizado.

7. Gestão de acesso físico aos recursos de TIC

O CTIC deve definir perímetros de segurança para proteger ambientes e ativos contra acesso físico não autorizado aos recursos de TIC, de acordo com as diretrizes a seguir:

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 CTIC 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 CTIC.

III. Estabelecer meios de controle de acesso físico a ambientes que não for conveniente a implementação de mecanismos de controle de acesso.

O acesso físico a ambientes seguros ou ativos de tratamento e armazenamento de dados da UFAM é destinado apenas a pessoal autorizado, devendo manter um processo de gestão de acessos para fornecimento, revisão periódica, atualização e revogação das autorizações, deve também implementar e manter seguro logs ou registro físico de todos os acessos aos ativos de informação.

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 CTIC;

III. Supervisionado e monitorado;

Os ativos de armazenamento e tratamento de dados que se encontrem fora da UFAM 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.

Será permitido o acesso restrito somente aos técnicos do CTIC devidamente identificados e habilitados, as seguintes dependências físicas:

a) Data Center: situado no prédio do CTIC do campus universitário e no bloco M do mini campus (site backup). Trata-se de pontos de controle de acesso físico considerados críticos.
b) Salas técnicas de redes de dados: situados nos prédios do campus universitário e nas unidades externas que participam da rede óptica da instituição. Trata-se de ambiente exclusivo, destinado apenas a abrigar os ativos físicos associados aos recursos de TIC.
c) Áreas técnicas de redes de dados: situados nos prédios do campus universitário e nas unidades externas que participam da rede óptica da instituição, em salas sob responsabilidade de setores administrativos diversos.

É de responsabilidade do CTIC a atualização de lista com a localização dos ativos físicos que suportam os recursos de TIC (ANEXO C).

É de responsabilidade dos setores que possuem salas com áreas técnicas, o controle de acesso aos ativos físicos que suportam os recursos de TIC, devendo o acesso ser autorizado somente aos técnicos do CTIC identificados e habilitados.

É de responsabilidade da PCU as providências pertinentes a garantir que nos projetos prediais os ativos físicos que suportam os recursos de TIC sejam abrigados preferencialmente em instalações técnicas dedicadas, isto é, salas técnicas ao invés de áreas técnicas, estabelecendo assim o isolamento apropriado a estes recursos, e portanto, mitigando o acesso físico não autorizado.

É ainda de responsabilidade da PCU as providências pertinentes ao monitoramento físico, vigilância digital e rondas de segurança a estes espaços físicos.

8. Auditoria e monitoramento

É de responsabilidade do CTIC e restrito a este o monitoramento da utilização dos recursos de TIC por parte dos usuários, podendo ainda exercer fiscalização nos casos de apuração de uso indevido desses recursos, bem como bloquear, temporariamente, sem aviso prévio, os recursos utilizados para atividades que coloquem em risco a segurança da informação, até que seja verificada a situação e descartada qualquer hipótese de dano à infraestrutura tecnológica da instituição.

É expressamente proibido o acesso ao conteúdo das informações armazenadas através dos recursos de TIC em situações diversas das previstas nesta política.

9. Disposições gerais

A rede institucional é considerada uma forma de comunicação oficial da Universidade Federal do Amazonas, e, portanto, deverá ser de uso restrito às atividades administrativas e acadêmicas.

Os serviços de TIC oferecidos pela UFAM, e mantidos pelo CTIC, deverão sempre que possível possuir sistema de credencial unificado (Single Sign On, SSO) combinada com MFA, de forma que o usuário deverá usar a mesma credencial (login, token, biometria, etc.) para obter acesso aos serviços oferecidos pela instituição.

A conta institucional é de uso pessoal e intransferível, sendo ela a forma de autenticação necessária para se obter acesso a diversos serviços, como:

- Sistemas acadêmicos e administrativos (portais UFAM, e-campus, SEI, sistemas em nuvem computacional, etc.);
- Sistemas de comunicação de dados (correio eletrônico, telefonia digital, videoconferência, dispositivos de acesso, workstations, intranet, Internet, rede sem fio, VPN, etc.);
- Plataformas online (ambientes virtuais de aprendizagem (AVA) e sistemas EAD, salas Classroom, biblioteca virtual, sistemas de armazenamento e compartilhamento de arquivos, fóruns de discussão, etc.;

Os usuários são responsáveis por garantir que suas atividades de acesso aos recursos de tecnologia estejam em conformidade com as políticas, normas e diretrizes estabelecidas na PoSIC UFAM, e devem informar qualquer incidente ou descumprimento da norma que afete a segurança das informações.

Quando houver suspeita de quebra da segurança da informação que exponha ao risco os serviços ou recursos de tecnologia, o CTIC junto a ETIR fará a investigação para que medidas adequadas possam ser tomadas para mitigar os danos, podendo interromper temporariamente o serviço ou área afetada, sem prévia autorização, visando proteger a integridade dos sistemas e dados.

O descumprimento das disposições da política de controle de acesso poderá acarretar medidas disciplinares, conforme estabelecido nas normas e regulamentos internos da universidade.

As medidas disciplinares podem incluir advertências, suspensões temporárias de acesso aos recursos de tecnologia, bloqueio, revogação, cancelamento, ou mesmo ações legais em casos graves de violação.

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 Tecnologia da Informação.

Quando houver suspeita de quebra da segurança da informação que exponha ao risco os serviços ou recursos de tecnologia, o Setor responsável pela Tecnologia da Informação ou Equipe de Tratamento e Resposta a Incidentes de Segurança fará a investigação, podendo interromper temporariamente o serviço afetado, sem prévia autorização.

I. Nos casos em que o autor da quebra de segurança for um usuário, o Setor responsável pela Tecnologia da Informação ou ETIR 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 omissas nas legislações correlatas será resolvida pelo Comitê de Governança Digital - CGD.

10. Revisão e Atualização

Esta política deverá ser revisada e atualizada anualmente ou conforme necessário para garantir sua relevância e assegurar as melhores práticas e conformidades frente às mudanças regulatórias e tecnológicas.

11. Vigência

Esta política entra em vigor na data de sua publicação.

i) ANEXO A - Modelo de Termo de Responsabilidade

SERVIÇO PÚBLICO FEDERAL

Universidade Federal do Amazonas

TERMO DE RESPONSABILIDADE

Pelo presente instrumento, eu _____, CPF _____, identidade _____, expedida pelo _____, em _____, e associado/lotado no(a)_____desta instituição, DECLARO, sob pena das sanções cabíveis nos termos da Política de Segurança da Informação e Comunicações da Universidade Federal do Amazonas e demais legislações vigentes que assumo a responsabilidade por:

I. Tratar o(s) ativo(s) de informação como patrimônio da Universidade Federal do Amazonas;
II. Utilizar as informações em qualquer suporte sob minha custódia, exclusivamente, no interesse do serviço da Universidade Federal do Amazonas;
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 Universidade Federal do Amazonas;
V. Responder, perante a Universidade Federal do Amazonas, 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 Política de Segurança da Informação e Comunicação (PoSIC) 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 em âmbito acadêmico ou profissional realizando as tarefas e operações, em estrita observância aos procedimentos, normas e disposições que rege o acesso à rede corporativa, computadores, Internet e/ou utilização de e-mail;

VIII. Não revelar, fora do âmbito acadêmico ou 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.

Manaus, AM, _____de _____de _____.

_____

Assinatura eletrônica / <Nome do usuário e seu vínculo acadêmico/setor organizacional>

_____

Comitê de Governança Digital (Nome da autoridade responsável pela autorização do acesso)

j) ANEXO B – Padrão de Formação de Endereços de Correio Eletrônico

Caixas Postais Individuais: <https://www.gov.br/governodigital/pt-br/governanca-de-dados/padrao-de-formacao-de-enderecos-de-correio-eletronico.pdf>

Definições: Para os efeitos desta norma, consideram-se as seguintes definições: Prenome: É o nome próprio ou nome de batismo, escolhido pelos pais por ocasião do registro de nascimento, para individualizar seu portador. Pode ser simples *(Luiz, Maria) ou composto (Luiz Carlos, Maria Regina).*

Sobrenome: É o segundo elemento fundamental do nome civil e é a porção do nome do indivíduo que está relacionada com a sua ascendência, também chamado de nome de família. O sobrenome será simples quando provir apenas do sobrenome materno ou paterno e composto quando provir de ambos.

Nome Social: É o prenome adotado e de identificação pela sociedade dos casos definidos pela *Portaria Nº 233 de 18 de maio de 2010, do Ministério do Planejamento, Orçamento e Gestão.*

Regra Padrão: A composição do endereço de correio eletrônico deverá obedecer à Regra Padrão devendo ser formada pelo primeiro prenome seguido de um *PONTO (.)* seguido do último sobrenome. A Regra Padrão para criação de endereço de correio eletrônico destina-se a uniformizar a sua estrutura, para que o destinatário de uma mensagem possa ser identificado e localizado de maneira rápida, única e segura.

Exemplo para *Luiz Carlos Fraga da Silva:*

luiz.silva@organização.gov.br

Exceções: Os casos abaixo definidos constituem as Regras para Exceção, devendo os usuários solicitar junto à área de TI do órgão, a utilização das mesmas para formação do endereço eletrônico.

(1) Existir um usuário homônimo previamente cadastrado no órgão;

(2) O usuário ser conhecido no seu meio social, inclusive profissional, pelo nome composto ou por outro sobrenome que não seja o definido pela regra padrão; ou

(3) Quando da utilização de nome social.

Regras para Exceção: Casos (1) e (2): o endereço de correio eletrônico deverá ser formado pelo prenome seguido de um *PONTO (.)* seguido por um sobrenome, conforme os

exemplos abaixo. No caso de prenome composto, a separação entre os nomes deverá ser feita por *HÍFEN (-)*.

Exemplos para *Luiz Carlos Fraga da Silva:*

luiz.fraga@organização.gov.br *luiz-carlos.fraga@organização.gov.br*

carlos.silva@organização.gov.br *luiz-carlos.silva@organização.gov.br*

carlos.fraga@organização.gov.br

Obs: Se o endereço de correio eletrônico formado já estiver em uso, deve-se adotar uma destas opções:

a) **Sobrenome** seguido de um *PONTO (.)* seguido por um **prenome**;

b) **Prenome** seguido de um *HÍFEN (-)* e do **sobrenome** seguido de um *PONTO (.)* seguido da primeira inicial do **prenome** e do **sobrenome**;

c) **Prenome** seguido de um *PONTO (.)* seguido do último **sobrenome** seguido de um número sequencial;

Exemplos para *Luiz Carlos Fraga da Silva:*

a) silva.luiz@organização.gov.br *c) luiz.silva.1@organização.gov.br*

b) luiz-silva.ls@organização.gov.br

Caso (3): o endereço de correio eletrônico deverá ser formado pelo **nome social** seguido de um *PONTO (.)* seguido por um **sobrenome**, conforme os exemplos abaixo. No caso de **nome social** composto, a separação entre os nomes deverá ser feita por *HÍFEN(-)*.

Exemplos para *Luiz Carlos Fraga da Silva (nome de batismo) / Carla Regina (nome social)*

carla-regina.silva@organização.gov.br *carla-regina.fraga@organização.gov.br*

Restrições: Devem ser observadas as seguintes restrições:

• Ser utilizado ponto "." apenas para separação do nome do sobrenome;

• Não é permitido o uso de apelidos, números, ou qualquer outra forma fora dos padrões disciplinados nesse documento;

• Não utilizar acentos (til, agudo, grave, circunflexo, trema);

• **Prenome**, simples ou composto, pode ter no máximo 16 caracteres, permitidos caracteres alfabéticos minúsculos, e hífen, sem espaços entre eles;

• **Sobrenome**, simples ou composto, pode ter no máximo 40 caracteres, permitidos caracteres alfabéticos minúsculos, e hífen, sem espaços entre eles.

k) ANEXO C – Localização dos ativos físicos associados aos recursos de TIC da Universidade Federal do Amazonas

l)

Campus Manaus

SETOR NORTE

Localização	**Tipo de instalação**
CTIC	Data center
Reitoria	Sala técnica
Reitoria	Sala técnica
Reitoria	Sala técnica
Centro de Convivência – RU	Sala técnica
FT - Biblioteca	Sala técnica
ICE-ICOMP1	Sala técnica
IFCHS01	Área técnica
IFCHS02	Área técnica
FACED01	Área técnica
FACED02	Área técnica
FACED03	Área técnica
Biblioteca Setorial Norte	Área técnica
FES - Administração	Área técnica
Bloco de salas de aula 09 - FES	Área técnica
Bloco de salas de aula 08 - FES	Área técnica
Bloco de salas de aula 07 - FES	Área técnica

Bloco de salas de aula 06 - FACED	Área técnica
Bloco de salas de aula 05 - FACED	Área técnica
Bloco de salas de aula 04 - FACED	Área técnica
Bloco de salas de aula 03 - IFCHS	Área técnica
Bloco de salas de aula 02 - IFCHS	Área técnica
Bloco de salas de aula 01 - IFCHS	Área técnica
FIC	Área técnica
IFCHS - Geo-história	Área técnica
IFCHS - Mario Ypiranga	Área técnica
FAARTES	Área técnica
FT - Salas de aula	Área técnica
FT - Design	Área técnica
FT - Robótica	Área técnica
FT - LIFT1	Área técnica
FT - CDEAM	Área técnica
FT - CETELI2	Área técnica
FT - CETELI1	Área técnica
FT - Administração	Área técnica
FT - Materiais	Área técnica
FT - Pós-graduação	Área técnica
FT - Geotecnia	Área técnica
FT - Transportes	Área técnica
FT - Saneamento	Área técnica

FT - LIFT2	Área técnica
FT - Mecânica	Área técnica
FT - Auditório	Área técnica
FT - Administração	Área técnica
FT - Tapauá	Área técnica
ICE - Matemática	Área técnica
ICE - Salas de aula	Área técnica
ICE - Estatística	Área técnica
ICE - Central Analítica	Área técnica
ICE - Química	Área técnica
ICE - ICOMP2	Área técnica
ICE - ICOMP3	Área técnica
ICE - Geociências	Área técnica
ICE - Física	Área técnica

SETOR SUL

Localização	**Tipo De Instalação**
Arqueologia	Sala técnica
FCA01	Sala técnica
FCA02	Sala técnica
Biblioteca Setorial Sul	Sala técnica
ICB02	Sala técnica
ICB01	Sala técnica

Posbioagro	Sala técnica
FAPSI	Sala técnica
Bloco M - CAM	Data Center
Sauim	Área técnica
Bloco J - FCA	Área técnica
Bloco H - ICB	Área técnica
Restaurante Universitário Sul	Área técnica
Buhrnheim	Área técnica
CAIS	Área técnica
FEFF - PROAMDE	Área técnica
Bloco B - FEFF Administração	Área técnica
FEFF – Vida Ativa	Área técnica
Bloco C - FEFF	Área técnica
FEFF - JuUFAM	Área técnica
FEFF – Idoso Feliz	Área técnica
Segurança do Campus	Área técnica
TV UFAM	Área técnica
ADUA	Área técnica
Eulálio Chaves	Área técnica
COMPEC	Área técnica
FCA - Sementes	Área técnica
FCA - Aviário	Área técnica
FCA - Viveiro	Área técnica

Patrimonio	Área técnica
Fábrica de Medicamentos	Área técnica
CDTECH	Área técnica
Laboratório de Mensuração de Carbono	Área técnica
Lapec	Área técnica
Bloco X - FAPSI	Área técnica
Bloco V - FCA	Área técnica
Bloco Z - FCA	Área técnica
Bloco U - FCA	Área técnica
Bloco T - CCA	Área técnica
PIATAM	Área técnica
ICB - Anatomia	Área técnica
Bloco C - FCA	Área técnica
FCF	Área técnica
Bloco D - ICB	Área técnica
Bloco E - ICB	Área técnica
Bloco G - CAM	Área técnica
Laboratório técnico de madeira	Área técnica
DEMAT	Área técnica
Prefeitura	Área técnica
PPGAS	Área técnica
CED	Área técnica

UNIDADES EXTERNAS

Localização	Tipo de Instalação
Jurídico	Sala técnica
Biblioteca Central	Sala técnica
Antiga FCF	Área técnica
Museu Amazônico	Área técnica
Caua2	Área técnica
Caua1	Área técnica
Faculdade de odontologia	Área técnica
Faculdade de medicina	Área técnica
Escola de enfermagem	Área técnica

Campus Itacoatiara

Prédio	Tipo de instalação
Bloco A	Área técnica
Bloco B	Área técnica
Bloco C	Área técnica
Bloco D	Datacenter
Bloco E	Área técnica

Campus Parintins

Prédio	Tipo de instalação
Bloco I	Sala técnica
Bloco II	Datacenter
Bloco III	Sala técnica

Campus Coari

Unidade 01

Prédio	Tipo de instalação
Bloco 01 – Pavimento Térreo	Data center
Bloco 02 – Pavimento Térreo	Área técnica
Bloco 03 – Pavimento Térreo	Área técnica

Unidade 02

Prédio	Tipo de instalação
Bloco único	Sala técnica

Campus Benjamin Constant (Alto Solimões)

Prédio	Tipo de instalação
Bloco 01	Sala técnica
Bloco 02	Data center
Bloco 03	Sala técnica
Bloco 04	Sala técnica

Campus Humaitá

Unidade nova

Prédio	Tipo de instalação

Bloco 01 – Pavimento Térreo	Área técnica
Bloco 02 – Pavimento Térreo	Datacenter

Unidade antiga

Prédio	**Tipo de instalação**
Bloco único	Área técnica