UNIVERSIDADE FEDERAL DO AMAZONAS
UFAM

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

DESENVOLVIDO POR:
COORDENAÇÃO DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES - CSIC/CTIC

Julho
2023

Universidade Federal do Amazonas
Centro de Tecnologia da Informação e Comunicação
Coordenação de Segurança da Informação e Comunicação

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.	Márcia de Paula e Gilberto Libania
25/07/2023	1.1	Revisão na Coordenação de Segurança da Informação e Comunicação.	Márcia de Paula e Gilberto Libania
-	1.2	Revisão nas Coordenações do CTIC.	-

Universidade Federal do Amazonas
Centro de Tecnologia da Informação e Comunicação
Coordenação de Segurança da Informação e Comunicação

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, 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) Lei nº 13.709, de 14 de agosto de 2018: institui a Lei Geral de Proteção de Dados Pessoais (LGPD).
b) 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.
c) 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.
d) Política de Segurança da Informação e Comunicação da Universidade Federal do Amazonas.
e) 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 o controle de acesso.

f) 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).
g) Norma ABNT NBR ISO/IEC 27002:2022: fornece diretrizes para práticas de gestão de segurança da informação e normas de segurança da informação para as organizações.

1.3. Das definições

Para os efeitos desta política, consideram-se:

h) 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;
i) 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;
j) 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;
k) 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;
l) 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);

m) 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);

n) 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;

o) 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;

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

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

r) 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;

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 (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 da UFAM. Esta política contempla o controle de acesso lógico à informação e aos recursos computacionais, bem como também abrange o controle de acesso físico das áreas e instalações de acesso restrito definidas nesta política.

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. 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.

São responsabilidades dos usuários dos recursos de TIC:

a) Manter as telas de seus dispositivos protegidas por bloqueio quando se afastarem deles 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;
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, caso ocorra ou perceba algum incidente de segurança ou violação de dados, 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 se ausentarem 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 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 da respectiva conta de acesso, e

2. 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), 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.

3. Gestão de acesso lógico

O acesso lógico aos recursos tecnológicos oferecidos deverá ser realizado pelo setor responsável pela gestão de acessos utilizando sistema de controle de acesso ou através de ofício encaminhado ao CTIC.

O setor responsável pela gestão de acessos é aquele responsável pelo vínculo do usuário com a instituição. Desta forma, o acesso deve ser concedido e mantido por estes

setores, baseado nas responsabilidades e tarefas de cada usuário e de acordo com as definições abaixo elencadas:

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

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 de empresas prestadoras de serviços, estagiários, alunos e demais usuários com vínculo institucional.

3.1. Criação de conta de acesso

As contas de cada perfil de usuário deverão ser administradas e autorizadas por meio do portal institucional e-Campus pelos respectivos gestores de acesso.

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 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.

3.1.1. Formação de nomes de usuário

As contas de acesso quanto ao seu padrão de formação para nomes de usuário 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.

3.1.2. Formação de senhas

O padrão adotado para o formato da senha 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 as seguintes regras:

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

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

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

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

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

3.1.3. 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 deve ser obrigatório para técnicos, docentes e estagiários, sendo facultado aos discentes.

.

3.1.4. 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 de cinco anos. Desta forma, mesmo

após o cancelamento do acesso lógico aos recursos, o período de cinco anos deve ser observado.

3.2. 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 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.

3.3. 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, os direitos de acesso aos recursos devem ser readequados pelo superior imediato e pelo setor responsável pela gestão de acesso. Os direitos de acesso antigos devem ser imediatamente revogados.

3.4. 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.

Na necessidade de utilização de login com privilégio de administrador por terceiros, o usuário deverá encaminhar 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.

3.5. 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 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.

4. Uso adequado do acesso

A conta de acesso aos recursos de TIC é pessoal e intransferível, sendo vedado o seu compartilhamento em qualquer hipótese.

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.

5. 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.
b) Edoc: repositório de documentos administrativos. Utilizado para armazenar, preservar, 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) [outras de acordo com definições do negócio];

6. Controle de acesso remoto

O acesso remoto deve ser realizado por meio de rede virtual privada (VPN) utilizando equipamentos de comunicação apropriados e dotados de mecanismos de segurança adequados visando garantir o acesso remoto seguro, tais como proteção de antivírus, firewall, 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.

7. 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 se trata 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.

8. Gestão de acesso físico aos recursos de TIC

O acesso físico aos recursos de TIC é permitido somente aos técnicos do CTIC, devidamente identificados e habilitados.

São de acesso restrito aos técnicos do CTIC as seguintes dependências físicas:

a) Data Center: situado no prédio do CTIC do campus universitário e no bloco M do minicampus (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.

9. 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.

h) 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)

i) 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>

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

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 - Geohistoria	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