



SERVIÇO PÚBLICO FEDERAL
MINISTÉRIO DA EDUCAÇÃO
Universidade Federal do Pampa

INSTRUÇÃO NORMATIVA UNIPAMPA Nº 14, 21 DE NOVEMBRO DE 2024

Regulamenta a gestão do controle de acesso, complementar à Política de Segurança da Informação e Comunicação – POSIC no âmbito da Universidade Federal do Pampa, Resolução Nº CONSUNI 284, de 28 de outubro de 2020,

O PRESIDENTE DO COMITÊ DE GOVERNANÇA DIGITAL, NA CONDIÇÃO DE GESTOR DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO, no uso de suas atribuições e tendo em vista o disposto no art. 27, inciso VII da Política de Segurança da Informação e Comunicação no âmbito da Universidade Federal do Pampa, Resolução CONSUNI Nº 284, de 28 de outubro de 2020,

CONSIDERANDO o Decreto Nº 12.069/2024, que dispõe sobre a Estratégia de Governo Digital 2024-2027, na sua íntegra;

CONSIDERANDO a Lei Nº 13.709/2018 – Lei Geral de Proteção de Dados, CAPÍTULO VII - Seção I – Art. 46; Seção II – Art. 50;

CONSIDERANDO o Decreto Nº 9.573/2018 - Política Nacional de Segurança de Infraestruturas Críticas (PNSIC), Anexo, Art. 3º, Inciso I;

CONSIDERANDO o Decreto Nº 9.637/2018 - Política Nacional de Segurança da Informação (PNSI), nos CAPÍTULO I - Art. 2º, Incisos III e IV; CAPÍTULO II - Art. 3º, Inciso XI; CAPÍTULO VI - Seção IV – Art. 15;

CONSIDERANDO o Decreto Nº 10.222/2020 - Estratégia Nacional de Segurança Cibernética (E-CIBER), Anexo, Itens 2.3.4 e 2.3.5;

CONSIDERANDO o Decreto Nº 10.046/2019 - Governança no Compartilhamento de Dados (GCD), Art. 2º, XXIII;

CONSIDERANDO a Instrução Normativa Nº 01/GSI/PR, Art. 12, Inciso IV, alínea "f";

CONSIDERANDO a norma ABNT NBR ISO/IEC 27002: 2013. Código de Prática para controles de Segurança da Informação, Itens 9 – 11.2.9 (Páginas 23 - 47);

CONSIDERANDO a 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);

CONSIDERANDO a norma ABNT NBR ISO/IEC 27701: 2019. Técnicas de segurança — Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação — Requisitos e Diretrizes, Itens 6 – 6.6.2 (Página 16);

CONSIDERANDO o Guia do *Framework* de Privacidade e Segurança da Informação (PPSI), Controles 5, 6, 12 e 31;

CONSIDERANDO a Instrução Normativa N° 04/GSI/PR, de 26 de março de 2020, Capítulo II;

CONSIDERANDO a Portaria GSI/PR N° 93, de 18 de outubro de 2021 em sua íntegra;

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

CONSIDERANDO a orientação GSI 09/2023. OSIC (ORIENTAÇÃO DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA) — Gestão de Acesso Privilegiado (*Privileged Access Management – PAM*) – parte 2 de 2., em sua íntegra;

R E S O L V E:

CAPÍTULO I

ESCOPO

Art. 1º. Esta norma Complementar de Gestão de Controle de Acesso objetiva estabelecer controles de identificação, autenticação e autorização para salvaguardar as informações da Unipampa, estejam elas em qualquer meio, seja digital ou físico, a fim de evitar a quebra da segurança da informação e quaisquer acessos não autorizados que implique em risco de destruição, alteração, perda, roubo ou divulgação indevida.

Art. 2º. Esta norma se aplica a todas as informações, nas qual Unipampa seja o agente de tratamento, ao meio utilizado para este tratamento, seja digital ou físico, e as dependências físicas desta instituição, bem como a qualquer pessoa que circule nas dependências ou que interaja exercendo controle administrativo, técnico ou operacional, mesmo que eventual, desses meios de tratamento, incluindo:

I - Todos os servidores, sejam efetivos ou temporários, da Unipampa;

II - Todos os contratados e terceirizados que acessam fisicamente as dependências ou que acessam a rede e sistemas de informação da Unipampa.

CAPÍTULO II

CONCEITOS E DEFINIÇÕES

Art. 3º. Para os efeitos desta norma, aplica-se os seguintes termos e definições:

I - acesso - ato de ingressar, transitar, conhecer ou consultar a informação, bem como possibilidade de usar os ativos de informação de um órgão ou entidade, observada eventual restrição que se aplique;

II - acesso remoto – a capacidade de conectar-se a rede corporativa da Unipampa a partir de um local

físico diferente, utilizando uma conexão à internet. Este tipo de acesso permite a um usuário institucional utilizar os sistemas institucionais informatizados, mesmo que esteja fora de um prédio da Unipampa;

III - 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;

IV - 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;

V - credenciais de acesso - informações que pertencem a um usuário e que são usadas para identificar e validar o acesso a qualquer recurso computacional com ou sem o uso de um dispositivo de identificação;

VI - sistemas institucionais informatizados – dispositivos físicos ou sistemas de informação institucionais usados para suportar ou automatizar processos internos de trabalho, como computadores ou sistemas de informação (ex.: Guri, SEI, Moodle);

VII - usuário - qualquer pessoa que possua ou não vínculo com a Unipampa, e que necessite de credenciais para acesso a um sistema ou Recurso Institucional Informatizado da Unipampa;

VIII - usuários externos - usuário que não contempla os requisitos de usuário institucional e que, consideradas as atividades finalísticas e administrativas da Unipampa, necessita acesso a Serviços de TIC institucionais de forma temporária, participantes de eventos, colaboradores ou prestadores de serviço cuja forma de relação temporária com a instituição preveja a necessidade de acesso por tempo limitado a um ou mais Serviços de TIC institucionais;

IX - usuários institucionais – usuário que, consideradas as atividades finalísticas e administrativas da Unipampa, necessita acesso a Serviços de TIC institucionais e que possui vínculo formal vigente com a Unipampa, temporário ou permanente (servidores, alunos e empregados temporários), conforme a situação do cadastro em módulos do SIE ou com vínculo ativo a outra instituição de ensino e pesquisa brasileira participante da federação CAFe - Comunidade Acadêmica Federada;

X- VPN (*Virtual Private Network*) – uma forma de acesso remoto na qual um túnel seguro na Internet, entre o dispositivo remoto e a rede corporativa da Unipampa, permite ao usuário acessar os sistemas institucionais informatizados estando fisicamente fora das dependências da Unipampa.

CAPÍTULO III

ACESSO LÓGICO

Art. 4º. O acesso lógico aos Sistemas Institucionais Informatizados será realizado por meio de sistema de controle de acesso. O acesso deve ser concedido e mantido pela DTIC, baseado nos perfis de cada usuário.

I - Terão direito a acesso lógico todos os usuários de recursos de tecnologia da informação.

II - O acesso remoto realizado por meio de VPN – Rede Virtual Privada, será concedido mediante autorizações.

Art. 5º. São adotadas técnicas de segmentação de rede visando limitar o acesso de forma eficiente e segura, assegurando que apenas usuários e dispositivos autorizados possam interagir com partes específicas da rede.

Art. 6º. A gestão de contas é centralizada por meio de serviço de diretório ou provedor de SSO (*single signon*).

CAPÍTULO IV

CREDENCIAIS DE ACESSO

Art. 7º. Todas as credenciais de acesso ou contas institucionais utilizadas na Unipampa tem de estar associadas a uma pessoa física e atreladas aos seus documentos oficiais reconhecidos pela legislação

brasileira.

Art. 8º. Para utilização em Sistemas Institucionais Informatizados, será obrigatório o uso de uma credencial de acesso, constituída por identificação única (login) e senha.

Art. 9º. A identificação biométrica ou equivalente, quando implementada, deve ser vinculada a uma conta institucional.

Art. 10. As credenciais de acesso ou contas institucionais são de uso pessoal e intransferível, sendo proibida a sua divulgação e compartilhamento, sob pena de serem bloqueadas se constatada qualquer irregularidade.

Art. 11. O padrão adotado para o formato da conta institucional de acesso do usuário institucional é a sequência primeiro nome + último nome do usuário, como por exemplo, mariasilva.

§ 1º. Nos casos de já existência de conta de acesso para outro usuário, será adotada outra combinação, utilizando parte do nome completo do usuário para o qual a conta está sendo criada.

§ 2º. Nos casos de nome social, o usuário poderá requisitar um padrão de nome de acesso que atenda este direito (de acordo com a Res. Nº 61/CONSUNI, de 29 de agosto de 2013).

Art. 12. O padrão adotado para o formato da conta institucional de acesso do usuário externo é o número de CPF.

Art. 13. O padrão adotado para o formato da senha institucional considera a quantidade mínima e máxima de caracteres, a tipologia (letras, número e símbolos) e a proibição de repetição de senhas anteriores. Parágrafo único. A formação da senha da identificação deve seguir as regras:

- a) deve conter de 8 (oito) a 20 (vinte) caracteres alfanuméricos (isso inclui todos os caracteres do teclado, exceto o espaço);
- b) Não são aceitas sequências (abcd, 1234, etc.) ou dados pessoais (nome, CPF, endereço, etc);
- c) A reutilização de senhas obedecerá a um ciclo mínimo de trocas.

Art. 14. Será fornecida uma senha temporária no momento da criação da conta, que deverá ser alterada pelo usuário no primeiro acesso.

Art. 15. As senhas institucionais possuem validade máxima de um ano.

§ 1º. O usuário poderá trocar ou recuperar uma senha esquecida a qualquer momento, por sistema de troca e recuperação de senha, disponibilizado pela DTIC.

§ 2º. A troca da senha será solicitada automaticamente antes do final do prazo de validade ou a qualquer momento, por motivo de segurança constatada pela ETIR.

§ 3º. Caso o usuário não efetue a troca no prazo estabelecido, seu acesso será bloqueado até que uma nova senha seja definida.

CAPÍTULO V

BLOQUEIO, DESBLOQUEIO E CANCELAMENTO DAS CREDENCIAIS DE ACESSO

Art. 16. A conta institucional será bloqueada nos seguintes casos:

- I. Após 5 (cinco) tentativas consecutivas de acesso malsucedidas;
- II. Em casos de determinação administrativa ou judicial;
- III. Quando da suspeita de mau uso dos serviços disponibilizados pela Instituição, descumprimento da Política de Segurança da Informação e Comunicação – POSIC ou normas correlatas em vigência;
- IV. Após tentativas de troca de senha sem sucesso;
- V. Caso o usuário não efetue a troca no prazo estabelecido.

Art. 17. O desbloqueio da conta institucional será realizado mediante solicitação formal nos casos dos incisos II e III do art. 16º e automaticamente após tempo estabelecido nos demais casos.

CAPÍTULO VI

CONTAS COM PRIVILÉGIO ADMINISTRADOR

Art. 18. A atribuição do perfil administrador às contas institucionais é permitida somente para usuários cadastrados para execução de tarefas específicas na administração de ativos de informação.

I. Somente Analistas e Técnicos em Tecnologia da Informação, devidamente identificados e habilitados, poderão ter perfil com privilégio de administrador nos equipamentos locais e ativos de rede.

II. A identificação (*login*) com privilégio de administrador em ambiente de laboratório será fornecida em caráter provisório, podendo ser renovada por solicitação formal do titular da unidade requisitante.

CAPÍTULO VII

RESPONSABILIDADES

Art. 19. São responsabilidades da DTIC:

I - Prover e manter o sistema de guarda, criação e alteração das credenciais dos usuários e contas de serviços;

II - Comunicar o usuário com antecedência quando da proximidade da expiração das credenciais;

III - Realizar o bloqueio das credenciais, conforme o disposto no Capítulo VI;

IV - Manter as senhas em sistema seguro e criptografado;

V - Monitorar a utilização de serviços de rede e Sistemas Institucionais Informatizados, podendo ainda exercer fiscalização nos casos de apuração de uso indevido desses recursos.

Art. 20. São responsabilidades dos usuários:

I - todos os acessos realizados através de suas credenciais de acesso e por possíveis danos causados por seu uso indevido;

II - guarda da conta e senha institucionais e demais credenciais de acesso, como *tokens*, chaves criptográficas etc.;

III - utilizar suas credenciais somente para fins designados e para os quais estiverem devidamente autorizados (de acordo com suas funções e responsabilidades);

IV - substituir senhas provisórias após o primeiro acesso ao sistema;

V - reportar imediatamente ao superior imediato e/ou à ETIR os casos de violação de credenciais, acidental ou não, e providenciar a sua substituição;

VI - realizar o uso correto perante a instituição e a legislação vigente das credenciais de acesso, de acordo com o art. 9º desta norma;

VII - solicitar o cancelamento das senhas quando não forem mais necessárias.

CAPÍTULO VIII

DISPOSIÇÕES GERAIS

Art. 21. Fica aprovada, no âmbito da Unipampa, a Norma Complementar de Gestão de Controle de Acesso, em complemento às diretrizes estabelecidas no artigo 24 da Política de Segurança da Informação e Comunicação - POSIC da Unipampa.

Art. 22. A Unipampa deve definir regras de limitação ou restrição de acesso aos usuários, para que estes

disponham de privilégios mínimos necessários para exercerem suas atividades, funções e responsabilidades pré-definidas.

Art. 23. Os casos omissos nesta norma serão tratados pelo Comitê de Governança Digital – CGD

Art. 24. Esta Instrução Normativa entra em vigor na data de sua publicação.

Bagé, 21 de novembro de 2024.

Edward Frederico Castro Pessano
Reitor



Assinado eletronicamente por **EDWARD FREDERICO CASTRO PESSANO, Reitor**, em 21/11/2024, às 09:48, conforme horário oficial de Brasília, de acordo com as normativas legais aplicáveis.



A autenticidade deste documento pode ser conferida no site https://sei.unipampa.edu.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1604020** e o código CRC **268BFB5E**.

Referência: Processo nº 23100.018124/2024-02

SEI nº 1604020