Política de controle de acesso à informação e aos recursos e serviços de TIC

UNIFESSPA | Centro de Tecnologia da Informação e Comunicação

Histórico de revisão

Versão	Data	Autor	Descrição
1.0	15/12/2020	Ralfh Alan Gomes Machado	Versão inicial
1.1	23/03/2021	Ralfh Alan Gomes Machado, Edney A. do Nascimento, Fernando Miranda, Idelvandro Fonseca, Vitor Castro	Revisão e sugestões
1.2	01/04/2021	CGD (Comitê de Governança Digital)	Consolidação final e aprovação no CGD

Apresentação

Este documento integra a Política de Segurança da Informação e Comunicação (PoSIC) da Universidade Federal do Sul e Sudeste do Pará (Unifesspa) e tem por finalidade estabelecer os objetivos, diretrizes e competências relacionadas ao controle de acesso à informação e aos recursos de tecnologia da informação. Esta política será aplicada, no que couber, às atividades de todos os usuários de recursos tecnológicos pertencentes ou gerenciados pelo Centro de Tecnologia da Informação e Comunicação (CTIC), incluindo servidores, colaboradores, consultores externos, estagiários e prestadores de serviço que exercem atividades no âmbito da Unifesspa ou quaisquer usuários que venham ter acesso a dados ou informações protegidos pela presente norma.

Capítulo I

Fundamentação legal e normativa

Art. 1º. A presente política está fundamentada nos seguintes instrumentos legais e normativos:

I – Lei nº 12.527, de 18 de novembro de 2011, que regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal, revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991, e dá outras providências;

II – Decreto nº 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação;

III – Decreto nº 7.724, de 16 de maio de 2012, que regulamenta a Lei nº 12.527, de 18 de novembro de 2011, que dispõe sobre o acesso a informações previsto no inciso XXXIII do caput do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição;

IV – ABNT NBR ISO/IEC 27001:2013, que trata dos sistemas de gestão da segurança da informação – requisitos;

V – ABNT NBR ISO/IEC 27002:2013, que estabelece o código de prática para controles de segurança da informação;

VI – Instrução Normativa nº 1, de 27 de maio de 2020 que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal.

VII – Instrução Normativa GSI nº 2, de 5 de fevereiro de 2013, que dispõe sobre o credenciamento de segurança para o tratamento de informação classificada, em qualquer grau de sigilo, no âmbito do Poder Executivo Federal;

VIII – Instrução Normativa GSI nº 3, de 6 de março de 2013, que dispõe sobre os parâmetros e padrões mínimos dos recursos criptográficos baseados em algoritmos de Estado para criptografia da informação classificada no âmbito do Poder Executivo Federal;

Capítulo II

Conceitos e definições

Art. 2º. Para os efeitos desta norma ficam estabelecidos os seguintes conceitos:

I – ativo: qualquer coisa que tenha valor para a organização [ISO/IEC 13335–1:2004];

II – autenticação: processo que busca verificar e confirmar a identidade do usuário;

III – confidencialidade: propriedade da informação que garante que a mesma não será disponibilizada ou divulgada a indivíduos, entidades ou processos sem autorização [ISO/IEC 13335–1:2004];

IV – acesso: ato ou permissão para ingressar, transitar, conhecer, consultar, manipular e utilizar os ativos de informação;

V – acesso privilegiado: acesso a ambientes restritos ou controlados e informações sensíveis;

VI – acesso restrito: acesso limitado ou controlado concedido sob condições específicas;

VII – análise de riscos: conjunto de procedimentos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os ativos de informação, mediante o equilíbrio dos custos operacionais e financeiros envolvidos;

VIII – ativos de informação: os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;

IX – classificação da informação: atribuição pela autoridade competente do grau de sigilo dado à informação, documento, material, área ou instalação;

X – Comitê de Gestão de Segurança da Informação e Comunicação (CGSIC): grupo de pessoas com a responsabilidade de assessorar a implementação das ações de segurança da informação e comunicações no âmbito da Unifesspa;

XI – controle de acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso à informação;

XII – gestão de segurança da informação e comunicação: ações e métodos que visam a integração das atividades de análise de riscos, gestão de continuidade do negócio, tratamento de incidentes, classificação e tratamento da informação, conformidade, credenciamento, segurança cibernética, física, lógica, de recursos humanos e documental aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto, à tecnologia da informação e comunicações;

XIII – gestor de segurança da informação e comunicações: responsável pelas ações de segurança da informação e comunicações no âmbito da Unifesspa;

XIV – gestor de sistema: servidor da Unifesspa designado formalmente para gerenciar sistema de informação, sendo responsável pelo ciclo de vida e projeto de melhoria do sistema sob sua responsabilidade; e

XV – informações sensíveis: ativos de informação que têm caráter privado ou possuem restrições quanto à sua publicação, cujo acesso indevido poderão gerar danos ou perdas à Instituição;

Capítulo III

Objetivos e diretrizes

Art. 3º Constituem objetivos da presente política:

I – garantir que o acesso físico e lógico à informação seja franqueado exclusivamente a pessoas autorizadas, com base nos requisitos de negócio e de segurança da informação;

II – estabelecer mecanismos e controles para garantir a efetiva proteção dos dados, informações e conhecimentos gerados;

III – reduzir os riscos de ocorrência de perdas, alterações e acessos indevidos aos ativos de informação;

IV – preservar a disponibilidade, integridade, confiabilidade e autenticidade das informações;

V – garantir o direito de acesso, considerando a classificação da informação produzida, as obrigações da legislação vigente e a análise de riscos existente;

VI – definir o nível de acesso baseado em normas internas e procedimentos formais específicos;

VII – revisar e controlar os acessos de forma periódica e manter o seu registro disponível para consulta individual ou de auditoria;

VIII – exigir procedimentos formais para o fornecimento de informações ou transferência de ativos físicos de áreas restritas para áreas de criticidade diferente de sua origem, segundo a classificação da informação e a análise de riscos existente; e

IX – elaborar normas internas ou procedimentos formais específicos para acessos por meio de dispositivos particulares que fizerem uso da infraestrutura da Unifesspa.

Art. 4º. Constituem diretrizes da presente política:

I – garantia de que os acessos aos ativos de informação sejam autorizados com base em níveis de restrições;

II – instituição de procedimentos prévios de credenciamento para a criação de contas de acesso e utilização de credenciais físicas para o acesso aos ativos de informação;

III – uso das credenciais de acesso de modo pessoal e intransferível, permitindo de maneira clara e inequívoca o reconhecimento do usuário;

IV – conscientização dos usuários sobre a necessidade de sigilo, conforme classificação da informação e características de chaves de acesso;

V – registro dos acessos aos ativos de informação da Unifesspa;

VI – existência de responsáveis formais pela concessão e manutenção dos acessos privilegiados;

VII – observância da legislação específica para a concessão e controle de acesso às informações sensíveis ou sigilosas;

VIII – utilização de ferramentas ou protocolos de proteção contra acesso não autorizado aos ativos de informação;

IX – distinção de acesso para servidores e público em geral;

X – bloqueio ao acesso e apuração da responsabilidade administrativa, penal e civil do usuário pelo uso indevido ou acesso não autorizado aos ativos de informação;

XI – revisão do acesso concedido aos usuários que tiveram mudança em suas atribuições, devendo ser readequados imediatamente ou bloqueados em caso de perda do vínculo com a Instituição;

XII – classificação dos ativos de informação de acordo com o valor, a criticidade, o tipo de ativo e o grau de sigilo das informações que podem ser tratadas em tais ativos, devendo ser mapeados aqueles considerados críticos;

XIII – difusão e exigência do cumprimento da presente Política e da legislação de regência do assunto;

XIV – identificação e avaliação sistemática dos riscos à segurança da informação e comunicações dos ativos de informação;

XV – definição de regras específicas para autorizar o acesso e o credenciamento dos usuários em conformidade com a classificação dos ativos de informação;

XVI – concessão de acesso aos ativos de informação restrita ao exercício das atividades do cargo, função ou atribuições de cada usuário; e

XVII – responsabilização do usuário pelas ações realizadas por meio de sua credencial de acesso.

Capítulo IV

Credenciais de acesso

Art. 5º. Os controles de acesso implementados na Unifesspa devem aplicar o princípio “necessidade de conhecer”, o qual prescreve a necessidade legítima que justifique o acesso à informação por pessoa, sistema ou entidade, bem como o princípio “privilégio mínimo”, o qual estabelece que o perfil de acesso concedido deve incluir tão somente os poderes necessários para o atendimento das legítimas necessidades.

Art. 6º. Os controles de acesso lógicos na organização devem utilizar, preferencialmente, autenticação com certificado digital ICP-Brasil, a fim de prover identificação inequívoca de pessoas físicas e jurídicas e comprovação de autoria em transações digitais.

Art. 7º. A credencial de acesso é formada pelo nome de usuário (*login*) e uma senha de acesso.

§1º O nome de usuário deve seguir a padronização estabelecida pelo CTIC.

§2º É dever do usuário alterar a sua senha após o primeiro acesso à rede corporativa ou quando solicitado pelo CTIC, seguindo as seguintes regras:

I – a senha de acesso deverá ser composta de no mínimo 08 (oito) caracteres, obrigatoriamente com a presença de letras e números;

II – não criar senhas óbvias baseadas em datas de aniversário e nascimento, nomes, apelidos, dentre outros;

III – não escolher senhas com caracteres idênticos consecutivos, todos numéricos

ou todos alfabéticos sucessivos;

IV – não escolher senhas baseadas em palavras contidas em dicionários;

§3º As credenciais de acesso são pessoais e intransferíveis.

§4º É vedado o compartilhamento de credenciais em qualquer situação, inclusive nas hipóteses de substituição temporária de função.

§5º Fica sujeito às penalidades, conforme disposto nos termos da lei, o usuário que fizer uso da credencial de outrem para acesso e utilização de ativos ou recursos de informática.

Art. 8º. Toda e qualquer ação executada pelo usuário utilizando suas credenciais de acesso será de responsabilidade exclusiva do mesmo, devendo este zelar pelos princípios de confidencialidade e das regras de boas práticas determinadas pela PoSIC, especialmente:

I – na utilização de computadores que não sejam fornecidos pela Unifesspa;

II – na utilização de redes de comunicação não fornecidas pela Unifesspa.

Art. 9º. Caso as credenciais de acesso tenham sido comprometidas, divulgadas ou descobertas, o usuário deverá informar imediatamente ao CTIC para que as medidas cabíveis sejam tomadas.

Art. 10º. Por medidas de segurança, após 05 (cinco) tentativas de autenticação sem êxito, a credencial de acesso à rede será bloqueada por 10 (dez) minutos e, caso ocorra um novo bloqueio, a credencial será bloqueada definitivamente.

Parágrafo único. O desbloqueio poderá ser realizado somente pelo CTIC.

Capítulo V

Do cadastro e permissões de usuários

Art. 11º. Para efeitos desta Norma, ficam estabelecidos os seguintes tipos de usuários:

I – servidores: servidores efetivos e comissionados da Unifesspa;

II – discentes: alunos vinculados à instituição;

III – estagiários: estagiários que possuem um contrato firmado com a Unifesspa;

IV – cedidos: funcionários cedidos por outros órgãos a Universidade, por meio de termo de convênio ou portaria, sejam eles funcionários efetivos, comissionados ou estagiários no órgão de origem;

V – terceiros: funcionários que prestam serviço para a Universidade através de um contrato firmado com a mesma;

VI – voluntários: prestadores de serviços voluntários, regulamentados pela Universidade;

VII – usuários de outros órgãos: usuários de outros órgãos que necessitem de acesso a algum sistema de informação da Unifesspa;

Art. 12º. O cadastro dos servidores e estagiários será realizado pelos próprios usuários.

§ 1º Compete à Pró–Reitoria de Desenvolvimento e Gestão de Pessoas (PROGEP), quanto ao cadastramento e alterações de dados dos servidores e estagiários, enviar ao CTIC, por meio de sistema automatizado ou, na ausência deste, por meio de comunicação oficial:

I – as alterações de dados cadastrais e inativações;

II – os afastamentos temporários e definitivos, bem como o retorno de afastamentos temporários;

III – no caso de servidores, as alterações de lotação e localização;

IV– no caso de estagiários, a data final do contrato de estágio que corresponderá à data de expiração das credenciais do usuário.

§ 2º A solicitação de concessão ou revogação de permissões de acesso deverá ser solicitada:

I – ao CTIC, pelo próprio servidor, respeitando as suas designações;

II – ao CTIC, pela chefia imediata do servidor ou estagiário;

III – a PROGEP, em casos excepcionais.

§ 3º Após a perda do vínculo do servidor com a Unifesspa, por aposentadoria ou exoneração, as credenciais serão mantidas somente para acesso ao contracheque, enquanto necessário, devendo ser posteriormente eliminadas.

§ 4º As mudanças de lotação, localização e afastamentos definitivos ou temporários de servidores e estagiários deverão ser comunicadas à PROGEP pela chefia imediata, para adequar a situação do usuário nos sistemas de gestão, cabendo a esta chefia o ônus por qualquer uso indevido da credencial do usuário decorrente da

não comunicação de algum dos eventos tratados neste parágrafo.

§ 5º As unidades ficarão responsáveis por manter o mapeamento de perfis dos sistemas/módulos da instituição, atribuindo-lhes as devidas responsabilidades através de documentos oficiais.

Art. 13º. O cadastro de funcionários cedidos de outros órgãos, que possuem convênio com a Unifesspa, será realizado pelo CTIC, mediante solicitação da PROGEP.

§ 1º Para que um funcionário cedido seja cadastrado é necessário que exista um convênio firmado entre os órgãos, com data de vigência que corresponderá à data de expiração das credenciais do usuário.

§ 2º Compete à PROGEP solicitar ao CTIC além do cadastro, a alteração e inativação de funcionários cedidos.

§ 3º O responsável pelo setor onde o funcionário cedido está alocado deve solicitar ao CTIC a concessão e a revogação de permissões para o usuário.

Art. 14º. O cadastro de terceiros, que prestam serviço para a Unifesspa através de um contrato firmado, será realizado pelo CTIC, mediante solicitação do gestor do contrato.

§ 1º Para os efeitos do cadastramento de terceiros, o gestor do contrato deverá informar até qual data o usuário deverá estar ativo, para que seja atribuída como data de expiração das credenciais do mesmo, não podendo ser posterior ao término da vigência do contrato.

§ 2º Compete ao gestor do contrato solicitar ao CTIC o cadastro, alteração e inativação de terceiros, além da concessão e revogação de permissões para o mesmo, de acordo com a necessidade do serviço.

Art. 15º. O cadastro de usuários de órgãos externos será realizado pelo CTIC, mediante solicitação do responsável sobre o convênio com o órgão.

§ 1º Para que um usuário de órgão externo seja cadastrado, é necessário que exista um convênio firmado entre os órgãos, com data de vigência que corresponderá à data de expiração das credenciais do usuário.

§ 2º Compete ao responsável do convênio com o órgão externo solicitar ao CTIC o cadastro, alteração e inativação dos usuários, além da concessão e revogação de permissões para os mesmos.

Art. 16º. O cadastro, alteração e inativação de servidores serão realizados pelos próprios, quando possível, ou pelo CTIC em caso contrário.

Art. 17º. Não serão realizados cadastros de usuários voluntários.

Art. 18º. Cabe ao CTIC realizar o bloqueio, preferencialmente de forma automática, dos usuários cuja data de expiração das credenciais tenha sido ultrapassada.

Art. 19º. O cadastro de usuários que não se enquadrem no descrito nesta política, serão realizados somente se houver procedimento formal criado pelo Gestor de Segurança da Informação que contemple este cadastro.

Art. 20º. As credenciais de acesso serão entregues pelo CTIC diretamente aos usuários.

Parágrafo único. A entrega das credenciais de acesso somente deverá ser realizada após o cadastro do usuário pela área competente no sistema de gestão utilizado para este tipo de usuário.

Art. 21º. É de responsabilidade do CTIC realizar os cadastros, alterações, bloqueios, concessões e revogações de acesso aos usuários internos da Unifesspa, de acordo com as necessidades funcionais e em conformidade com as informações constantes nos sistemas utilizados pela PROGEP, sendo permitido acesso exclusivamente aos recursos e sistemas necessários à execução de suas atividades funcionais, podendo ser realizado de forma automática baseado na localização e no tipo de usuário.

Capítulo VI

Da recuperação de senhas

Art. 22º. Em caso de perda de senha de acesso aos serviços de TIC da Unifesspa, o usuário, ou a chefia imediata do mesmo, deverá solicitar ao CTIC a recuperação da senha.

§ 1º O procedimento de recuperação de senhas pelo CTIC só deverá ser utilizado quando:

I – o recurso disponibilizado não oferecer procedimento automático de recuperação de senha;

II – o procedimento automático de recuperação de senha não puder ser completado.

§ 2º Quando a recuperação de senha for solicitada pela chefia imediata, o CTIC notificará, por meio de correio eletrônico institucional da chefia, a conclusão do procedimento e a nova senha temporária de acesso.

§ 3º O usuário deverá alterar a senha fornecida imediatamente após o procedimento.

Capítulo VII

Disposições finais

Art. 23º. Os casos omissos na presente norma serão resolvidos pelo Comitê de Governança Digital.

Art. 24º. Esta Norma entra em vigor na data de sua publicação.