MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL FLUMINENSE
CONSELHO UNIVERSITÁRIO

RESOLUÇÃO CUV/UFF Nº 308, DE 06 DE MARÇO DE 2024

Dispõe sobre a Política de Segurança da Informação (PSI) da Universidade Federal Fluminense (UFF).

O CONSELHO UNIVERSITÁRIO DA UNIVERSIDADE FEDERAL FLUMINENSE, no uso de suas atribuições estatutárias e regimentais, e o que mais consta do Processo nº 23069.178579/2023-21,

R E S O L V E :

Art. 1º - **Aprovar** a Política de Segurança da Informação (PSI) da Universidade Federal Fluminense (UFF).

Art. 2º - A presente Resolução entrará em vigor na data da sua aprovação.

* * * *

Sala das Sessões, 06 de março de 2024.

FABIO BARBOZA PASSOS
Presidente
# # # # # #

Anexo I

Política de Segurança da Informação (PSI) da Universidade Federal Fluminense.

Capítulo I Disposições Preliminares

Art.1º A Política de Segurança da Informação (PSI) tem como objetivo estabelecer mecanismos e controles para garantir a efetiva proteção dos dados, informações e conhecimentos gerados, redução dos riscos de ocorrência de perdas, alterações e acessos indevidos, preservando a produção intelectual, disponibilidade, integridade, confiabilidade e autenticidade das informações, na UFF.

Art. 2º A administração e gestão da segurança da informação em ambiente computacional da UFF ficarão a cargo da Superintendência de Tecnologia da Informação – STI da UFF.

Art. 3º A Superintendência de Tecnologia da Informação (STI) será a responsável pelas normas e procedimentos institucionais que se façam necessários para a garantia da Segurança e mitigação de riscos ao ambiente de Tecnologia da Informação – TI da UFF.

Art. 4º Esta PSI se aplica a toda a comunidade acadêmica da UFF e seus órgãos, nos diversos níveis hierárquicos e vínculos – membros, servidores e demais agentes públicos ou particulares que, oficialmente,executem atividades vinculadas à atuação institucional da UFF – que, a qualquer momento, tenham necessidade de utilizar os recursos de TI.

Art. 5º A Superintendência de Tecnologia da Informação (STI) e o Comitê de Segurança da Informação (CSI), deverão manter uma lista de responsabilidades pelas aprovações dos variados tipos de liberações deacesso.

Art. 6º A Superintendência de Tecnologia da Informação será responsável pela edição e aplicação dos planos de gerenciamento e resposta a incidentes de segurança da informação em ambientes computacionais da UFF, devendo os mesmos ser suportados por política, norma ou procedimento específicos para tal.

Parágrafo único. Todos os servidores e demais colaboradores que tratem de gerenciamento de sistemas, acesso à informação e atividades relacionadas à segurança da informação são co-responsáveis pela execução dos planos, políticas e procedimentos de segurança da informação, bem como por mitigar incidentes de segurança da informação e agir com celeridade para notificação e resolução dos mesmos.

Art. 7º Os servidores deverão ser capacitados para o desenvolvimento de competências em privacidade e segurança da informação, com a devida comunicação aos níveis estratégico, tático e operacional da UFF.

Capítulo II
Das Definições e Categorizações

Art. 8º As redes, compostas pelos seus ambientes, salas de equipamentos, e demais ativos, serão categorizadas conforme sua criticidade quanto à segurança da informação, para que sejam aplicadas as políticas descritas conforme a criticidade. Os níveis sugeridos são

1. Redes em ambientes públicos (alunos, salas de aula, espaços comuns, espaços de convivência, etc.)
2. Redes em ambientes com dados sensíveis (laboratório com pesquisas sensíveis, setores administrativos,secretarias acadêmicas, etc.)
3. Redes em ambientes com controle compartilhado (por projeto acadêmico ou institucional)
4. Redes em ambientes dos sistemas críticos (núcleo de servidores e virtualização)

Art. 9º Para efeito desta política, considera-se:

Ambiente computacional da UFF: inclui todos os recursos computacionais da UFF e recursos computacionais de usuários que, de alguma maneira, estejam utilizando a infraestrutura da rede da UFF;

Ambiente de Produção: ambiente que possui os dados reais dos sistemas, aqueles que os usuários utilizam para as funções diárias e cujas informações possuem valores legais e são aproveitadas pela instituição; porpossuir dados reais, é considerado ambiente extremamente crítico para a segurança das informações da instituição e, por isso, seu acesso deve ser limitado e somente liberado a quem realmente possui necessidadede utilizá-lo em tarefas do dia-a-dia e de alimentação de dados e informações para o sistema.

Ambiente de Homologação: ambiente no qual são feitos os testes em sistemas por um grupo restrito de usuários com acesso para validação de funções de um novo sistema ou de novas funções para um sistema preexistente; possui cópias desatualizadas dos dados de produção; por possuir dados reais, mesmo que desatualizados, existe razoável criticidade quanto ao comprometimento da segurança das informações institucionais.

Ambiente de Desenvolvimento: é o ambiente no qual os desenvolvedores de sistemas possuem acesso para criar um novo sistema ou novas funções para um sistema preexistente; obrigatoriamente possui esquemas reais (tabelas, campos em tabelas, com formatos e valores), porém, preenchidos com dados falsos; não compromete a segurança das informações da instituição.

Área Normativa: área da instituição que é responsável pelas informações contidas em um sistema; o usuárionormativo deve obrigatoriamente pertencer à área normativa.

Comunidade acadêmica: nesta política, considera-se como o conjunto de pessoas formado pelos alunos, ex-alunos, professores, técnico-administrativos e demais funcionários a serviço da instituição, bem como usuários dos serviços administrativos e acadêmicos da universidade e/ou dos recursos de informação e ambiente computacional.

Continuidade de negócios: capacidade estratégica e tática de um órgão ou entidade de se planejar e responder a incidentes e interrupções de negócios, minimizando seus impactos e recuperando perdas de ativos da informação das atividades críticas, a fim de manter suas operações em um nível aceitável, previamente definido. (PORTARIA GSI/PR nº 93/2021)

Incidente de segurança da informação: um ou múltiplos eventos de segurança da informação relacionados e identificados que podem prejudicar os ativos da organização ou comprometer suas operações. [FONTE:ISO/IEC 27035-1:2016, 3.4]

Perfil de acesso: conjunto de regras e privilégios de computação que liberam apenas determinadas operações em um sistema; é o perfil de acesso que determina as permissões de um usuário, ou seja, o que ele pode ou não fazer em um sistema.

Recursos computacionais da UFF: todos os ativos, incluindo sistemas, serviços e infraestrutura de TI,

independentemente de terem sido adquiridos pela instituição; uma vez integrantes de algum ambiente computacional, estão sujeitos a esta PSI.

Segurança da Informação: preservação da confidencialidade, integridade e disponibilidade da informação.[FONTE: ISO 27000:2020]

Sistema de informação: conjunto de aplicações, serviços, ativos (3.1.2) de tecnologia da informação ou outros componentes de manuseio de informações. [FONTE: ISO/IEC 27000:2018, 3.35]

Usuário: qualquer pessoa, com ou sem conhecimento especializado, que utilize os recursos computacionais e/ou o ambiente computacional da UFF.

Usuário Normativo: usuário de área, ou seja, não é necessariamente um analista de TI, que possui conhecimento profundo da área operacional e recebe conhecimento acerca dos perfis de usuário de um determinado sistema; é ele o responsável por aprovar a liberação de acesso de um determinado perfil de acesso a um determinado usuário; ou seja, é ele o responsável por afirmar que as funções de um determinadousuário são compatíveis com o perfil a ser liberado para o mesmo.

Capítulo III
Das Diretrizes Gerais

Art. 10º A segurança da informação é responsabilidade de qualquer usuário, não apenas da área de TI; destaforma, deverá refletir em hábitos, atitudes, responsabilidade e cuidados constantes no momento do uso, solicitação de aprovação de recursos etc.

Art. 11º O CSI irá propor projetos e ações para orientar e conscientizar os usuários quanto aos preceitos desegurança da informação a serem observados por todos, inclusive nas divisões, órgãos e campi da UFF quepossuem ambiente de TI distinto, com maior ou menor integração com o restante da instituição.

Art. 12º A utilização de informações e recursos computacionais deve ser sempre compatível com a ética, confidencialidade, legalidade e finalidade das atividades desempenhadas pelo usuário.

Art. 13º A utilização de recursos (ativos) disponibilizados pela instituição, ou integrados ao ambiente computacional, deve ser feita segundo os padrões e procedimentos definidos pela STI, através dos canais oficiais da STI, visando manter a disponibilidade e o desempenho das aplicações.

Art. 14º A utilização indevida dos recursos computacionais ou violação desta PSI será investigada e analisada pelas áreas competentes quanto a sua criticidade, e poderá provocar a suspensão temporária dos acessos, e deverá ser notificada à STI e à chefia imediata ou instância superior.

Art. 15º A UFF deverá manter um Plano de Gestão de Riscos com base na legislação vigente, que contemplea privacidade e a segurança da informação, as ameaças mais prováveis e suas ocorrências, a classificação dos riscos e medidas para tratamento.

Art. 16º A STI deverá manter um Plano de Contingência que permita operar os sistemas e recursos de forma que garanta um nível mínimo de disponibilidade de operação e deverá passar por revisões conforme necessidades técnicas.

Art. 17º A informação, documentação e produção técnica e acadêmica desenvolvidas e/ou inseridas nos

sistemas em uso na UFF são para uso exclusivo da Universidade para administração, gestão, prestação de serviços, ensino, pesquisa e extensão, sendo propriedade intelectual da Universidade e compartilhadas apenas com o Governo Federal, nos termos da lei.

Art. 18º A documentação dos sistemas de informação e projetos desenvolvidos devem ser disponibilizadasem meios de informação não perecíveis a longo prazo, no mínimo enquanto os sistemas estiverem em operação.

Art. 19º Os sistemas de informação e automação desenvolvidos, implementados ou integrados por terceiros deverão contemplar em seus contratos as cláusulas de proteção de dados e segurança da informação previstas em lei.

Art. 20º Todos os gestores de unidades deverão manter à disposição de suas equipes planos de contingênciaatualizados para os casos de queda de energia, inconformidades de acesso, de interrupção dos sistemas de informação e serviços de forma a não vulnerabilizar a segurança da informação.

Art. 21º Compete à alta administração, aos órgãos, departamentos, Comitês e Comissões delegadas monitorar o desempenho e avaliar a concepção, a implementação e os resultados da sua política de segurança da informação e das normas internas de segurança da informação;

Capítulo IV
Do acesso, classificação e tratamento das informações e proteção de dados

Art. 22º O acesso às informações institucionais deverá ser garantido ao usuário solicitante, nos termos da Lei geral de acesso à informação, desde que não infrinja o direito à privacidade, segurança pública, segurança institucional e legislações vigentes, sem que haja concessão de acesso aos sistemas em que a informação solicitada está registrada ou aos bancos de dados institucionais e desde que seja solicitado oficialmente, de acordo com os procedimentos para a prestação deste serviço e na forma da lei.

Art. 23º As informações classificadas como Reservada; Secreta e Ultrassecreta cumprirão os prazos de restrição de acesso previsto em lei, bem como aquelas as sigilosas por força de lei ou de contrato, as que requerem alto grau de controle e proteção contra acessos não autorizados, em segredo de justiça e hipótesesde segredo industrial decorrentes da exploração direta de atividade econômica pelo Estado ou por pessoa física ou entidade privada que tenha qualquer vínculo com o poder público.

PARÁGRAFO ÚNICO. É responsabilidade do produtor da informação, documento ou sistema providenciar a classificação das informações sensíveis e sigilosas e outras providências para garantir a restrição do acesso.

Art. 24º Todo e qualquer dado pessoal terá garantia de proteção e acesso restrito nos termos da lei, sendo acessível exclusivamente para as finalidades administrativas e acadêmicas da UFF.

Capítulo V
Da gestão da Segurança das Informações e suas responsabilidades

Art. 25º A responsabilidade pela gestão da segurança da informação é atribuída aos agentes envolvidos noprocesso de criação, salvaguarda, transporte e destruição da informação, sendo assim caracterizados:

I) Normativos: responsáveis pela classificação da informação, pela definição de perfil do usuário e o tipo de acesso às informações;

II) Usuários: todos aqueles que utilizam os recursos de tecnologia da informação, sendo, portanto, responsáveis pelo conhecimento e aplicação desta PSI;

III) Custodiante: responsável pela guarda da informação com segurança; na UFF e nos seus campi, esse agente é a Superintendência de Tecnologia da Informação, que terá a incumbência de implementar e controlar as autorizações de acesso à rede, correio/e-mail, internet, sistemas, servidores etc.; monitorar o uso adequado dos recursos liberados, bem como implementar e operacionalizar os mecanismos de segurança da informação.

Art. 26º Os usuários normativos de sistemas que não sejam da competência e expertise da atuação da STI,serão designados pela chefia de primeiro nível das áreas usuárias ou Comissões e Comitês instituídos pelo reitor e áreas legalmente responsáveis pelo sistema.

Art. 27º Os gestores das unidades organizacionais da UFF são usuários normativos das informações pertencentes ao domínio de sua autoridade, e podem delegar as funções de concessão de direitos de acesso/homologação de alterações nos sistemas; para tanto, devem formalizar estas delegações junto à Superintendência de Tecnologia da Informação.

Art. 28º É responsabilidade da área produtora da informação o monitoramento de obsolescência e providências para mudança de suporte, garantia de acesso, salvaguarda e preservação da informação, até orecolhimento para o arquivo permanente.

Capítulo VI
Das Vedações E Responsabilidades

Art.29º É vedada aos usuários a saída ou entrada de recursos computacionais institucionais de um setor sem prévia autorização do gestor responsável de cada unidade envolvida; apenas a STI possui autorização paramovimentação livre dos recursos computacionais institucionais.

Art. 30º É vedado o pernoite de recursos computacionais institucionais em veículos oficiais fora dos *campi* da Universidade ou em veículos privados de qualquer natureza, exceto quando autorizado por gestor competente.

Art. 31º É vedada a retirada de recursos computacionais de armazenamento de dados ou a mobilização dosmesmos sem autorização prévia dos gestores da STI responsáveis pela área.

Art.32º É responsabilidade do portador dos recursos computacionais autorizado a movimentá-los a garantia de proteção contra roubos, furtos e acesso indevido às informações e senhas porventura disponíveis no dispositivo.

Capítulo VII Ambientes Públicos

Art. 33º É permitido exclusivamente o uso de softwares licenciados nos equipamentos, dispositivos ou sistemas que estejam conectados e/ou em uso para quaisquer funcionalidades a serviço da instituição.

Art. 34º Equipamentos e sistemas com senha padrão, que vem junto com o produto, deve ser obrigatoriamente modificada pelo usuário antes da disponibilização do equipamento, sistema e/ou ambiente.

Art. 35º Todas as senhas são pessoais e intransferíveis.

Art. 36º A Superintendência de Tecnologia da Informação definirá e adotará um padrão de identificação de usuários que permitirá associar, de maneira única, cada direito de acesso à pessoa que o detém e concederá direitos de acesso compatíveis com as funções desempenhadas pelos usuários, através de perfis de acesso diferenciados; tais perfis objetivam restringir os dados e operações disponíveis, e sua definição será realizada em conjunto com Usuários Normativos.

Art. 37º A aquisição e instalação de equipamentos de rede devem obrigatoriamente atender às especificações técnicas definidas e publicadas pela STI.
Parágrafo único: Quando o equipamento pretendido não estiver previsto ou com suas especificações técnicas definidas pela STI, uma consulta formal prévia deve ser efetuada.

Art. 38º Equipamentos que necessitem ser conectados na rede UFF, exceto computadores, impressoras, scanners e similares, deverão ser registrados na STI, em especial switches e roteadores. A ausência do registro poderá culminar no bloqueio automático do acesso à rede pelo equipamento, sem aviso prévio.

Capítulo VII Ambientes Sensíveis

Art. 39º Todas as regras anteriores se aplicam a este ambiente.

Art. 40º É proibida a desinstalação, sem autorização formal dos órgãos responsáveis, de softwares ou hardwares que estejam sendo utilizadas para realizar controle físico e lógico dos recursos disponíveis; caso isso ocorra, o fato será comunicado, imediatamente, à chefia imediata do usuário ou ao Coordenador de curso do aluno e à STI, que irá apurar as causas, corrigirá o problema e providenciará a reinstalação.

Art. 41º A aquisição e instalação de softwares devem ser obrigatoriamente autorizadas pela STI.

Capítulo IX Ambientes compartilhados

Art. 42º Todas as regras anteriores se aplicam a este ambiente.

Art. 43º A STI, em parceria com o gestor do ambiente compartilhado, irá restringir as pessoas que poderãoser administradoras das respectivas estações de trabalho.

Capítulo X
Da Segurança Física de Ambientes Computacionais de Nível Crítico de TI

Art. 44º Todas as regras anteriores se aplicam a este ambiente.

Art. 45º Toda movimentação de equipamentos que compõem a estrutura de ambientes computacionais de nível crítico da UFF deve ser devidamente autorizada pela STI.

Art. 46º A UFF manterá dispositivos de proteção contra problemas de segurança física (condições ambientais adversas, desastres naturais, incêndios etc.) e lógica (vírus, acesso não autorizado, invasões etc.)compatíveis com os requisitos definidos nesta política; cabe à STI a definição de tais dispositivos de proteção, considerando características regionais, a criticidade das informações e os recursos tecnológicos envolvidos; nenhum fluxo de informações poderá existir sem que passe pelas camadas de proteção lógica.

Art. 47º Será utilizado hardware que disponha de recursos de redundância de processador, disco, energia etc., bem como equipamentos de prevenção e combate a incêndios (SPCI), além de controle da energia elétrica (rede estabilizada), temperatura e umidade.

Art. 48º O acesso físico aos Ambientes Computacionais de Nível Crítico de TI será restrito a pessoas oficialmente autorizadas.

Capítulo XI
Da Segurança Lógica de Ambientes Críticos de TI

Art. 49º Cabe à Superintendência de Tecnologia da Informação garantir que todos os ambientes lógicos (sistemas operacionais, SGDBs e sistemas de informação) tenham o seu acesso restrito por senhas, estandoem conformidade com as diretrizes descritas nesta Política.

Art. 50º Todo programa ou transação desenvolvido ou adquirido para execução em ambientes computacionais de nível crítico da UFF deve, obrigatoriamente, conter as verificações de autorização de execução em perfeita sintonia com o ambiente tecnológico em que será processado; não haverá exceção à verificação de autorização para execução de qualquer programa ou transação; em princípio, tudo que não for explicitamente permitido, está negado.

Art. 51º Todo novo programa ou transação adquirido para execução em ambientes computacionais de nível crítico da UFF deverá ser submetido à análise da Superintendência de Tecnologia da Informação com a finalidade de verificar sua conformidade.

Art. 52º Nenhuma senha será gravada no código-fonte de programas em texto plano, ou em arquivos ou tabelas destinadas a outros fins, devendo o tratamento desse tipo de informação seguir norma específica daSuperintendência de Tecnologia da Informação.

Art. 53º O acesso – mesmo que de simples consulta – aos arquivos ou tabelas de senha não será permitido,em nenhuma circunstância, a nenhum colaborador; tal restrição será provida por mecanismos de segurançalógica ou criptografia.

Art. 54º Toda conta de acesso a ambientes computacionais de nível crítico sem uso há mais de 60 dias até o limite de 180 dias poderá ser desabilitada pela Superintendência de Tecnologia da Informação, sem prévia autorização do proprietário ou da gerência para isso, de modo a liberar recursos físicos e/ou licenças de softwares alocados.

Art. 55º Somente será permitido o uso de recursos homologados e autorizados pela STI, desde que sejam identificados individualmente, inventariados, com documentação atualizada e atendendo a legislação pertinente em vigor.

Art. 56º A homologação de recursos computacionais em ambientes de nível crítico será de única e exclusivacompetência da STI, sendo regida por normas e procedimentos específicos de Homologação de Software eHomologação de Hardware.

Art. 57º É recomendada a existência de planos de segurança e de infraestrutura para implantação de sistemas de informação.

Art. 58º Não serão implementados sistemas de informação em ambientes computacionais de nível crítico quando trouxerem fragilidades que comprometam a segurança do ambiente UFF.

Art. 59º As senhas de acesso aos sistemas são de uso pessoal e intransferível;

Art. 60º Qualquer tentativa de acesso a sistemas cujo acesso lhe é negado, serão notificadas à chefia imediata do usuário.

Art. 61º É dever de todos zelar pelo sigilo de suas senhas de autenticação, bem como escolher senhas fortesdificultando serem descobertas facilmente por outra pessoa.

Art. 62º A conta de acesso e a senha de acesso para cada pessoa será única, individual e intransferível, sendo reconhecidas como equivalentes à sua assinatura e representam o nível de delegação concedida parao desempenho de suas funções.

Art. 63º Os acessos externos a recursos de ambiente de nível crítico da instituição somente serão concedidos mediante autorização prévia dos gestores responsáveis da STI, segundo instruções detalhadas caso a casoe realizados por intermédio de soluções técnicas institucionais.

Art. 64º O acesso à internet é permitido por intermédio de sistema de segurança institucional; é proibido o acesso direto à internet por intermédio de provedores externos estando conectado à rede UFF.

Art. 65º A Superintendência de Tecnologia da Informação deve assegurar que nenhum colaborador ou prestador de serviço obtenha direitos de acesso a recursos em ambientes de nível crítico, incompatíveis com a sua função, onde cada usuário terá uma única conta de acesso por aplicação, com permissões necessáriasapenas à execução de suas atividades.

Art. 66º Os colaboradores externos à UFF, mesmo não existindo vínculo direto, também poderão ser cadastrados nos sistemas, associados a um servidor responsável e também controlados por data de vigênciade acordo com a permanência na função.

Capítulo X
Da Segregação de Ambientes de desenvolvimento e suas Funções

Art. 67º A STI deve assegurar que todos os sistemas de informação da Instituição sejam aderentes às diretrizes a seguir:

I) Segregação de ambientes lógicos, com acessos únicos e isolados, de maneira que o ambiente de produçãofique apartado dos demais.

II) Os ambientes de teste, de homologação, de desenvolvimento e outros com funções similares, devem terseus códigos e dados (banco de dados) com acesso exclusivo dos usuários envolvidos com atividades de desenvolvimento e suporte a sistemas;

III) Estes usuários poderão realizar operações de consulta nos ambientes de produção, conforme necessidade e a critério da STI.

IV) O acesso às bases de dados dos ambientes de produção será feito, unicamente, através dos sistemas deinformação, estando completamente vetado qualquer tipo de acesso direto; os casos extremos de necessidade de liberação serão aprovados pela STI em conjunto com o usuário com nível gerencial da áreasolicitante.

V) Todo objeto, tais como programas, telas, funções etc., que for transferido para o ambiente de produção, deverá ser originado do ambiente de desenvolvimento ou de homologação, mantendo nesses ambientes o arquivo fonte original.

VI) Deve existir nos ambientes de produção, sempre que tecnologicamente possível, um controle automático das versões dos programas-fonte; este controle possibilitará a recuperação de versões anteriores,assim como a identificação do responsável pela sua implantação; o acesso aos programas-fonte, principalmente para inclusão, exclusão e alteração nos seus códigos, será restrito, através de perfis de acessoespecíficos e registrado em trilhas de auditoria.

Capítulo XI
Da política de backup e continuidade de negócios

Art. 68º A política de cópia de segurança e restauração de dados e sistemas será definida pela Superintendência de Tecnologia da Informação em documento específico, disponibilizado ao público apósaprovação oficial, bem como as normativas e regulamentações das atividades relacionadas;

Art. 69º As áreas normativas dos sistemas manterão cópias de segurança dos dados e sistemas de acordo com a política específica por tema acordada sobre backup.

Art. 70º Os backups de dados e sistemas devem ser realizados com nível de segurança física e lógica compatíveis com a criticidade e importância do conteúdo, atendendo aos requisitos legais

Art. 71º A STI é responsável por regulamentar os procedimentos para cópia de segurança e restauração dedados e sistemas e outros procedimentos de backup de dados nas redes em ambientes dos sistemas críticos.

Art. 72º Nos demais ambientes, a área normativa deverá providenciar responsáveis para a execução, acompanhamento e manutenção dos procedimentos de backup e restauração de dados e sistemas, de acordocom o art. 68°.

Art.73º A alta disponibilidade de acesso deve ser promovida por redundância adicional para conectividadede rede, obtida por meio de múltiplas rotas, passando por diferentes meios físicos.

Capítulo XII
Das Auditorias e Trilhas de Auditoria

Art. 74º Os órgãos oficiais de controle interno e externo poderão ter acesso a qualquer informação que esteja armazenada em ambiente lógico (Sistemas Operacionais, SGDBs e Sistemas de Informações)

Art. 75º Havendo evidência de qualquer atividade que possa comprometer a segurança do ambiente de TI, a UFF poderá auditar e monitorar as atividades de qualquer usuário, além de inspecionar seus arquivos e registros de acesso, sempre que julgar e comprovar necessidade.

Art. 76º A STI deve providenciar os recursos tecnológicos de seus sistemas e exigir recursos para que os sistemas de terceiros mantenham trilhas de auditoria sempre disponíveis para uso, bem como definir o tempo de retenção e as informações que deverão sistematicamente e automaticamente compor os

arquivosconhecidos como trilhas de auditoria.

Art. 77º As trilhas de auditoria de um determinado sistema devem ser de fácil acesso e, sempre que possível,centralizadas.

Art. 78º As trilhas de auditoria devem ser obrigatórias e registrar automaticamente todas as operações críticas efetuadas, sendo constituídas de, pelo menos, os seguintes campos:

I) Identificador do usuário (nominal, não podendo ser somente IP ou MAC Address),
II) Data da operação,
III) Horário da operação,
IV) Operação realizada,
V) Quando pertinente, quais dados foram modificados.

Art. 79º As trilhas de auditoria devem estar disponíveis para consulta por um prazo mínimo estipulado na legislação vigente.

Art. 80º As trilhas de auditoria não podem ser, em hipótese alguma, alteradas manualmente; as únicas inclusões de dados admissíveis serão as oriundas das rotinas automáticas de registro.

Capítulo XIII Referências Normativas

Art. 81º Esta PSI está alinhada aos instrumentos normativos apresentados a seguir:

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27001:2022.** Segurança da informação, segurança cibernética e proteção à privacidade. Sistemas de gestão da segurança da informação. Requisitos. ABNT: Rio de Janeiro, 2022.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27002:2022.** Segurança da informação, segurança cibernética e proteção à privacidade. Controles de segurança da informação. ABNT:Rio de Janeiro, 2022.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27005:2023**. Segurança da informação, segurança cibernética e proteção à privacidade. Orientações para gestão de riscos de segurançada informação. ABNT: Rio de Janeiro, 2023.

BRASIL. Casa Civil. Instituto Nacional de Tecnologia da Informação. **Instrução Normativa n. 07**, de 29de maio de 2020. Altera o tempo de armazenamento dos logs, trilhas de auditorias e imagens. Disponível em: https://www.gov.br/iti/pt-br/assuntos/legislacao/instrucoes-normativas/sei_iti_-_0427993_-_instrucao_normativa_07_2020.pdf Acesso em: 28 jun. 2023.

BRASIL. **Decreto n. 9.637**, de 26 de dezembro de 2018. Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação. Disponível em:

http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9637.htm Acesso em: 26 jun. 2023. BRASIL. **Decreto 7.845,** de 14 de novembro de 2012. Regulamenta procedimentos para credenciamentode segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleode Segurança e Credenciamento.

BRASIL. **Lei n. 13.709**, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponívelem: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm Acesso em: 31 maio 2023.

BRASIL. **Lei 9.609,** de 19 de fevereiro de 1998. Dispõe sobre a propriedade intelectual de programa de computador, sua comercialização no país e dá providências.

BRASIL. Gabinete de Segurança Institucional. **Instrução Normativa GSI/PR n. 01** de 27 de maio de 2020. Dispõe sobre a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências.

BRASIL. Gabinete de Segurança Institucional. **Portaria GSI/PR n. 93**, de 18 de outubro de 2021. Aprovao glossário de segurança da informação. Disponível em: <https://www.in.gov.br/en/web/dou/-/portaria-gsi/pr-n-93-de-18-de-outubro-de-2021-353056370> Acesso em: 13 set. 2023

BRASIL. Gabinete de Segurança Institucional. **Portaria GSI/PR n. 120**, de 21 de dezembro de 2022. Aprova o Plano de Gestão de Incidentes Cibernéticos para a administração pública federal. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-gsi/pr-n-120-de-21-de-dezembro-de-2022-452767918 Acesso em: 13 set. 2023

BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos/Secretaria de Governo Digital. **Portaria SGD/MGI nº 852**, de 28 de março de 2023. Dispõe sobre o Programa de Privacidade e Segurança da Informação (PPSI). Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-sgd/mgi-n-852-de-28-de-marco-de-2023- 473750908 Acesso em: 29 jun. 2023.

BRASIL. Programa do Governo Eletrônico Brasileiro. **Padrões de Interoperabilidade do Governo Eletrônico**: e-Ping, versão 2018. Disponível em: https://eping.governoeletronico.gov.br/ Acesso em: 05 jul. 2023.

BRASIL. Secretaria de Logística e Tecnologia da Informação. **Portaria Normativa SLTI/MP n. 05**, de 14 de julho de 2005. Institucionaliza os Padrões de Interoperabilidade do Governo Eletrônico – e-Ping.

[NBR] BRITISH STANDARD. **ISO/IEC 27000:2020**. Information technology – Security techniques – Information security management systems – Overview and vocabulary. Brussels: BS, 2020.