PORTARIA N.º 57.200 de 21 de setembro de 2016.

Aprova os termos contidos no documento Política de Segurança da Informação (PSI) da Universidade Federal Fluminense (UFF), aprovado pelo Comitê de Tecnologia da Informação (COTI), reformulado pela portaria n . º 44 . 709, de 23/05/2011 .

O VICE-REITOR DA UNIVERSIDADE FEDERAL FLUMINENSE NO EXERCÍCIO DA REITORIA, no uso de suas atribuições legais, estatutárias e regimentais,

Considerando o que determina o inciso VII do art. 5º IN GSI n.º 01, de 13 de junho de 2008 e observadas as diretrizes do Decreto nº 3.505, de 13 de junho de 2000 e a Norma Técnica ABNT NBR ISO/IEC 17.799:2005;

Considerando a necessidade de revisão periódica desta Política de Segurança da Informação visando a sua adequação aos preceitos definidos pelos órgãos de controle interno do Governo Federal;

Considerando, ainda, a relevância dos trabalhos de publicação dos documentos emitidos pela Universidade Federal Fluminense,

RESOLVE:

Art. 1º **Aprovar** os termos contidos nesta Política de Segurança da Informação (PSI) da Universidade Federal Fluminense, em anexo, aprovada pelo Comitê de Tecnologia da Informação (COTI), em reunião de 06/09/2016.

Art. 2º - Este documento sobre a Política de Segurança da Informação da Universidade está alinhado ao Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC), aprovado pela PORTARIA N.º 56.243 de 17 de maio de 2016.

Art. 3º Fica revogada a PSI anterior, publicada pela PORTARIA N.º 47.106 de 13 de junho de 2012, BOLETIM DE SERVIÇO - ANO XLII - N.º 106 - SEÇÃO II, págs. 121 a 134.

Publique-se, registre-se e cumpra-se.

ANTONIO CLAUDIO LUCAS DA NOBREGA
Vice-Reitor no Exercício da Reitoria

Assinado digitalmente por ANTONIO CLAUDIO LUCAS DA NOBREGA.
Documento Nº: 4481-6533 - consulta à autenticidade em https://sistemas.uff.br/sigaex/autenticar.action

Anexo

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

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 disponibilidade, integridade, confiabilidade e autenticidade das informações, na UFF.

Esta PSI da Universidade Federal Fluminense (UFF) tem seus termos aprovados conforme segue:

Art. 1º As questões relativas à segurança da informação, bem como a administração e gestão da segurança da informação em ambiente computacional da UFF ficarão única e exclusivamente a cargo da área de segurança da informação da Superintendência de Tecnologia da Informação – STI da UFF.

Art. 2º A área de segurança da informação da STI será a responsável pela edição de políticas, 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. 3º A aprovação e promulgação de normas e procedimentos de segurança da informação institucionais ficarão a cargo do Comitê de Tecnologia da Informação (COTI), enquanto para políticas ficará a cargo do Gabinete do Reitor da UFF.

Art. 4º Esta PSI se aplica a todos os colaboradores 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 Esta PSI deverá obrigatoriamente sofrer revisões, no mínimo uma vez a cada ano-calendário, visando à garantia de sua atualização, sempre condizente com as melhores práticas de segurança, as novas ameaças, a evolução tecnológica da UFF, seu crescimento, e constantes mudanças.

Art. 6º A área de segurança da informação da STI, juntamente com a representação jurídica da UFF e o Comitê de Tecnologia da Informação, deverá definir uma matriz de responsabilidades referente às aprovações e aos aprovadores no âmbito de TI, devendo esse documento ser revisado no mínimo uma vez em cada ano-calendário; essa matriz deverá obrigatoriamente contemplar os variados tipos e eventos de liberações de acesso e os respectivos responsáveis por sua aprovação; os usuários responsáveis deverão ser comunicados e estar cientes que, além da aprovação, poderão ser diretamente responsabilizados ou corresponsabilizados acerca de eventos de mau uso, descumprimento de normas ou, ainda, infrações legais originadas de autorizações oferecidas pelos mesmos.

Art. 7º Os processos, políticas, normas e procedimentos de gestão de riscos em segurança da informação deverão ser definidos pela Área de Segurança da Informação da STI e revisados periodicamente, no mínimo uma vez a cada ano-calendário.

Art. 8º A área de segurança da informação da STI será responsável pela edição e aplicação dos planos de gerenciamento e resposta a incidentes, devendo os mesmos ser suportados por política, norma ou procedimento específicos para tal, bem como chancelados pelo COTI.

Capítulo I
Das Definições

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

I) Ambiente Computacional: é o conjunto de recursos computacionais separado para uma determinada função. Subdividido em:

I.i) 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; por possuir 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 necessidade de utilizá-lo em tarefas do dia a dia e de alimentação de dados e informações para o sistema.

I.ii) 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.

I.iii) 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.

II) 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.

III) 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 determinado usuário são compatíveis com o perfil a ser liberado para o mesmo.

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

Art. 10 - Compõem os recursos computacionais da UFF equipamentos integrantes de quaisquer ambientes computacionais supracitados, sejam estes de quaisquer tipos ou finalidades (computadores, notebooks, telefones, switches, hubs, impressoras, periféricos etc.), independentemente de terem sido adquiridos pela instituição; uma vez integrantes de algum ambiente computacional, estão sujeitos a esta PSI.

Capitulo II
Das Diretrizes Gerais

Art. 11 A segurança da informação deve ser responsabilidade de todos, não apenas da área de TI; desta forma, deverá refletir em hábitos, atitudes, responsabilidade e cuidados constantes no momento do uso, solicitação de aprovação de recursos etc.

Art. 12 A STI irá providenciar os recursos humanos e materiais necessários para implementação das diretrizes estabelecidas nesta PSI, bem como orientar os usuários quanto às suas ações que serão tomadas, além de divulgar os preceitos de segurança da informação a serem observados por todos, inclusive nas divisões, órgãos e campi da UFF que possuem ambiente de TI distinto, com maior ou menor integração com o restante da instituição.

Art. 13 A utilização de informações e recursos computacionais deve ser sempre compatível com a ética, confidencialidade, legalidade e finalidade das atividades desempenhadas pelo usuário.

Art. 14 A utilização de recursos (sistemas, correio eletrônico, espaço em disco, equipamentos etc.) disponibilizados pela instituição, ou integrados ao ambiente computacional desta (rede e afins), deve ser feita segundo os padrões e procedimentos definidos pela STI, visando manter a disponibilidade e o desempenho das aplicações.

Art. 15 A conexão de equipamentos de terceiros na rede da instituição somente será permitida se não apresentar risco ao ambiente corporativo e estiver de acordo às políticas da instituição aplicáveis aos demais equipamentos, bem como houver sido analisada e declarada adequada pela STI.

Art. 16 As informações classificadas como confidenciais e/ou reservadas, bem como aquelas que necessitem de sigilo por força de lei ou contrato, requerem alto grau de controle e proteção contra acessos não autorizados, e são candidatas naturais à obtenção dessa classificação; o direito de acesso a estas informações requer autorização expressa do usuário normativo e é regida por política específica de classificação da informação.

Art. 17 A utilização indevida dos recursos computacionais pode provocar sanções a serem definidas pela STI e sua área de segurança da informação, dentre elas a suspensão dos acessos, e deve ser notificada à área de segurança da informação.

Art. 18 Qualquer violação dessa PSI constitui base para uma medida disciplinar, inclusive o término do contrato empregatício, conforme Política Disciplinar, bem como às sanções previstas por lei.

Capitulo III
Da Classificação das Informações

Art. 19 A classificação das informações na UFF será regulamentada por política específica acompanhada de procedimentos específicos de manipulação, salvaguarda, transporte, criação e edição.

Parágrafo único - Toda informação criada no ambiente da UFF não classificada explicitamente será considerada como informação reservada.

Capítulo IV
Da gestão da Segurança das Informações e suas responsabilidades

Art. 20 A responsabilidade pela gestão da segurança da informação é atribuída aos agentes envolvidos no processo 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 área de segurança da informação da STI, 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. 21 Os usuários normativos de natureza específica serão designados pelos de 1º nível de reporte das áreas usuárias.

Art. 22 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 área de segurança da informação da STI.

Capitulo V

Da Segurança Física do Ambiente de TI

Art. 23 Toda movimentação de equipamentos que compõem a estrutura do ambiente computacional da UFF, tais como servidores, roteadores, switches, hubs, controladores, impressoras, meios óticos e magnéticos de backup, e computadores, deve ser devidamente autorizada e registrada pela Divisão de Atendimento Técnico da STI.

Art. 24 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. 25 Para os sistemas classificados como de missão crítica, 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 corrente elétrica (rede estabilizada), temperatura e umidade e acesso físico e lógico restrito.

Capitulo VI
Da Segurança Lógica do Ambiente de TI

Art. 26 Cabe à área de segurança da informação da STI garantir que todos os ambientes lógicos (sistemas operacionais, SGDBs e sistemas de informação) tenham o seu acesso restrito por senhas, estando em conformidade com as diretrizes descritas nesta Política, salvo em situações nas quais existam restrições técnicas impeditivas que serão analisadas pela área de segurança.

Art. 27 Todo programa ou transação desenvolvido ou adquirido para execução no ambiente 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. 28Todo novo programa ou transação adquirido para execução no ambiente computacional da UFF deverá ser submetido à análise da área de segurança da informação da STI com a finalidade de verificar sua conformidade.

Art. 29 Nenhuma senha pessoal será gravada no código-fonte de programas, tampouco em arquivos ou tabelas destinadas a outros fins, devendo o tratamento desse tipo de informação seguir norma específica da STI para desenvolvimento e/ou aquisição de sistemas, softwares e afins.

Art. 30 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 segurança lógica ou criptografia.

Art. 31 Toda conta de acesso sem uso há mais de 60 dias até o limite de 180 dias poderá ser desabilitada pela área de segurança da informação da STI, sem prévia autorização do proprietário ou da gerência para isso, de modo a liberar recursos físicos e/ou licenças de softwares alocados; a exceção a esta regra é para usuários com primeiro nível de reporte à Reitoria, que serão contatados antes de o recurso ser desabilitado.

Art. 32 É proibida a desinstalação, nas estações usuárias, de softwares ou hardwares que são utilizadas para realizar controle físico e lógico dos recursos disponíveis; caso isso ocorra por procedimento indevido, o fato será comunicado, imediatamente, à chefia imediata do usuário e à Divisão de Atendimento Técnico, que apurará as causas, corrigirá o problema e providenciará a reinstalação.

Art. 33 Somente será permitido o uso de recursos homologados e autorizados pela Instituição, desde que sejam identificados individualmente, inventariados, com documentação atualizada e atendendo a legislação pertinente em vigor; a utilização destes sem licenças correspondentes é crime, previsto na Lei 9.609, de 19 de Fevereiro de 1998; portanto, qualquer usuário que exponha a Instituição a sanções jurídicas por utilização de softwares não homologados, independentemente de sua classificação (shareware, freeware, demo etc.) sem respaldo das respectivas licenças, estará sujeito às medidas disciplinares previstas, bem como às sanções previstas por lei.

Art. 34 A homologação de recursos computacionais será de única e exclusiva competência da STI, sendo regida por norma e procedimento específicos de Homologação de Software e Homologação de Hardware.

Art. 35 Nenhum software, independentemente de suas condições comerciais, será instalado ou baixado para equipamentos da UFF pelo próprio usuário, cabendo esta tarefa exclusivamente aos técnicos alocados nas gerências, coordenações e divisões da STI, que têm essa atividade inclusa no seu papel funcional; a exceção a esta regra somente poderá ocorrer mediante aprovação expressa da área de Segurança da STI, respeitando-se as premissas desta política; tais liberações terão sempre efeito pontual e nunca serão vistas como permanentes e genéricas.

Art. 36 A STI irá restringir as pessoas que poderão ser administradoras das respectivas estações de trabalho.

Art. 37 No caso de contas de acesso standard e impossíveis de serem eliminadas ou alteradas, as senhas standard (que vêm junto com o produto) serão, obrigatoriamente, modificadas imediatamente após a disponibilização do sistema e/ou ambiente, sem que haja solicitação específica sobre isso.

Art. 38 É obrigatória e existência de planos de segurança e de infraestrutura para implantação de sistemas de informação, sendo que não serão implementados se trouxerem fragilidades que comprometam a segurança do ambiente UFF.

Capitulo VII
Do uso e formação das senhas

Art. 39 Uma senha segura possui ao menos oito caracteres, inclui uma combinação de letras, números e símbolos e é fácil de ser lembrada, mas difícil de ser “quebrada”. Para a formação das senhas, serão adotados os seguintes critérios:

I) Tamanho mínimo de 8 caracteres

II) Nunca podem ser nulas ou estar em branco

III) Nunca visíveis na tela onde são informadas para atualização ou login IV) Nunca podem começar com os 3 caracteres iniciais do ID

V) Mínimo de 2 dígitos numéricos

VI) Mínimo de 2 caracteres alfanuméricos

VII) Impedir a repetição de um mesmo caractere 3 vezes seguidamente VIII) Vetar a reutilização de últimas 5 senhas utilizadas

IX) Serem bloqueadas após 5 tentativas consecutivas e malsucedidas de acesso

X) Passar por rotinas de crítica que impeçam a utilização de senhas “fracas” ou “facilmente quebráveis”

XI) Evitar palavras dicionarizadas

Art. 40 Todas as senhas expirarão independentemente da vontade dos usuários, no máximo, a cada 365 dias; além disso, todas as senhas iniciais – definidas pela área de segurança da informação da STI quando da liberação do acesso – serão expiradas e, ao primeiro acesso de cada usuário, será forçada a sua troca.

Art. 41 As senhas pessoais podem ser trocadas pelo próprio usuário, independentemente da sua data de expiração; porém, deverão ser impossibilitadas de serem trocadas mais de 1 vez no mesmo dia.

Art. 42 Nenhum colaborador poderá usar de sua ascendência hierárquica ou funcional sobre outrem para determinar ou obrigar que este compartilhe sua senha pessoal de acesso com quem quer que seja; o usuário que porventura receba esse tipo de solicitação deve comunicar o fato à área de segurança da informação da STI.

Art. 43O compartilhamento de senhas individuais é proibido para todos os níveis da instituição; da mesma forma, é também proibido abrir uma conexão autenticada para deixar que outra pessoa a utilize; em hipótese alguma, um usuário poderá passar sua senha pessoal de acesso para outrem; tal ação, uma vez detectada, terá classificação de gravidade em função do ambiente em que ocorreu e será devidamente reportada aos superiores hierárquicos dos usuários e à Pró-Reitoria de Gestão de Pessoas – PROGEPE.

Art. 44 Qualquer tentativa de “quebrar” (tentar descobrir) a senha pessoal de acesso de outra pessoa, ou mesmo invadir ambientes ou sistemas cujo acesso lhe é negado, serão notificadas à chefia imediata do usuário, e poderá resultar em medidas disciplinares apropriadas, conforme disposto na Política Disciplinar.

Art. 45 É dever de todos zelar pelo sigilo de suas senhas de autenticação, bem como escolher senhas fortes dificultando serem descobertas facilmente por outra pessoa.

Capitulo VIII
Da Segurança de Acessos

Art. 46 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 para o desempenho de suas funções.

Art. 47 Os acessos externos a recursos da instituição (acesso remoto de colaboradores, terceiros, fornecedores, clientes, e outros casos que vierem a surgir) somente serão concedidos mediante autorização prévia, segundo instruções detalhadas caso a caso e realizados por intermédio de soluções técnicas institucionais.

Art. 48 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. 49 Eventuais interligações entre redes (de forma física e/ou lógica) envolvendo processo de automação e/ou informação somente deverão ocorrer utilizando soluções corporativas definidas pela STI, de forma a garantir a disponibilidade, a integridade e a confidencialidade dos ambientes.

Capitulo IX
Do Controle de Acesso

Art. 50 A área de segurança da informação da STI deve assegurar que nenhum colaborador ou prestador de serviço obtenha direitos de acesso incompatíveis com a sua função, ou seja, cada usuário terá uma única conta de acesso por aplicação.

Art. 51 A área de segurança da informação da STI 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. 52 No caso de fiscais de outros órgãos públicos, mesmo não existindo vínculo direto, as pessoas também poderão ser cadastradas nos sistemas, associadas a um colaborador responsável e também controladas por data de vigência lógica.

Capitulo X
Da Segregação de Ambientes e Funções

Art. 53 A STI deve assegurar que todos os sistemas de informação da Instituição sejam aderentes às diretrizes a seguir:

I) Segregação de ambientes lógicos, de maneira que o ambiente de produção fique apartado dos demais.

II) Os ambientes que não sejam de produção – ou seja, de teste, de homologação, de desenvolvimento e outros – devem ser de acesso exclusivo dos usuários envolvidos com atividades de desenvolvimento e suporte a sistemas; estes usuários, nos ambientes de produção, podem efetuar, no máximo, operações de consulta.

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

IV) 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.

V) 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 recentes (dentro dos 6 meses predecessores e das 6 últimas versões), assim como a identificação do responsável pela sua implantação; o acesso aos programas-fonte, principalmente de inclusão, exclusão e alteração nos seus códigos, será restrito, através de perfis de acesso específicos e registrado em trilhas de auditoria.

Capitulo XI
Do Plano de Contingência

Art. 54 Para enfrentar situações de interrupção dos sistemas de informação, com consequente paralisação das atividades da UFF, o STI deverá manter um Plano de Contingência que permita operar os sistemas e recursos de forma que garanta um nível mínimo de operação.

Art. 55 O Plano de Contingência deverá passar por revisões periódicas, no mínimo uma vez a cada ano-calendário.

Art. 56 O Plano de Contingência deverá ser exercitado no mínimo 2 vezes ao ano.

Capitulo XII
Da Propriedade Intelectual

Art. 57 Todos os sistemas, projetos e/ou configurações desenvolvidos para atender as necessidades e os interesses da Instituição são de propriedade única e exclusiva da UFF, e somente poderão ser cedidos, comercializados ou distribuídos mediante a aprovação da

STI; esta regra deve ser formalizada em todos os contratos com fornecedores e prestadores de serviço ou atividades de desenvolvimento realizadas pela equipe de desenvolvimento da UFF.

Art. 58 - A documentação dos sistemas de informação e projetos desenvolvidos deve ser disponibilizada em meio ótico ou magnético, contendo:

I) Códigos-fonte dos objetos (programas, telas, transações, etc.) desenvolvidos;

II) Manual do Usuário e/ou Help On-Line, desde que apresente explicações sobre funcionalidades e não apenas preenchimento de campos;

III) Diagrama de Contexto e Especificação Funcional; IV) Diagrama de Casos de Uso e Casos de Uso; V) Dicionário de Dados (DD);

VI) Diagrama de Fluxo de Dados (DFD) ou Modelo de Transição de Dados (em projetos de automação, são indispensáveis os dois);

VII) Modelo de Entidade-Relacionamento (MER) ou Modelo de Objetos; VIII) Diagrama de Classes;

IX) Quaisquer outros artefatos de projeto e desenvolvimento gerados pela metodologia de projeto e desenvolvimento empregada no projeto.

Art. 59 - No caso dos sistemas de informação e automação desenvolvidos, implementados ou integrados por terceiros, a STI exigirá em contrato a disponibilização e atualização da documentação pertinente; os pagamentos a serem efetuados ao fornecedor estarão condicionados à entrega de tal documentação, que poderá ser proporcional aos produtos entregues em cada fase do projeto.

Capitulo XIII
Da Auditoria e das Trilhas de Auditoria

Art. 60 A Auditoria poderá ter acesso a qualquer informação que esteja armazenada em ambiente lógico (Sistemas Operacionais, SGDBs e Sistemas de Informação); havendo evidência de qualquer atividade que possa comprometer a segurança do ambiente de TI, pode a Auditoria auditar e monitorar as atividades de qualquer usuário, além de inspecionar seus arquivos e registros de acesso, sempre que julgar e comprovar necessidade.

Art. 61 A STI deve providenciar os recursos tecnológicos para que as trilhas de auditoria sempre existam e fiquem disponíveis para uso, bem como definir o tempo de retenção e as informações que deverão sistematicamente e automaticamente compor os arquivos conhecidos como trilhas de auditoria.

Art. 62 As trilhas de auditoria de um determinado sistema devem ser centralizadas, evitando a sua dispersão em vários arquivos, e ser de fácil acesso a quem de direito.

Art. 63 As trilhas de auditoria devem registrar automaticamente todas as operações críticas efetuadas, e

serão constituídas de pelo menos os seguintes campos:

I) Identificador do usuário (nominal, não podendo ser somente IP ou MAC Address), Data da operação, Horário da operação, Operação realizada, Dados antes da operação e dados após a operação.

Art. 64 - Sempre que surgir um novo ambiente lógico na instituição, a STI tomará a iniciativa de reunir-se com os Usuários Normativos correspondentes para deliberar sobre a criação das trilhas de auditoria.

Art. 65 - As trilhas de auditoria devem estar disponíveis para consulta por um prazo mínimo de 1 (um) ano, além de protegidas contra inclusão, exclusão ou alteração de dados; as únicas inclusões de dados admissíveis serão as oriundas das rotinas automáticas de registro.

Capitulo XIV
Referências Normativas

Art. 66 Esta PSI está alinhada aos instrumentos normativos apresentados a seguir:

I) Decreto 3.505 de 13 de julho de 2000 – Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal.

II) Decreto 7.845 de 14 de novembro de 2012 - Regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento.

III) 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.

IV) Instrução Normativa GSI/PR nº 01 de 01 de julho de 2008 – Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências.

V) Norma Complementar nº 03 de junho de 2009 à Instrução Normativa GSI/PR nº 01 – Recomenda diretrizes para elaboração de Política de Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal.

VI) e-Ping – Padrões de Interoperabilidade do Governo Eletrônico, de 16 de dezembro de 2008.

VII) Portaria SLTI/MP nº05 de 14 de julho de 2005 – Institucionaliza os Padrões de Interoperabilidade do Governo Eletrônico – e-Ping.

VIII) ABNT NBR ISO/IEC 27001:2013 – Sistema de Gestão de Segurança da Informação.

IX) ABNT NBR ISO/IEC 27002:2013 – Código de Práticas para Gestão de Segurança da Informação.