PSI – Política de Segurança da Informação

Documento de Diretrizes e Normas Administrativas

Elaborado por:
Tarcizo S. Santos
Assistente de Patrimônio
Decreto 8451/GAB/PM/JP/2017
(Responsável pela área de TI do FPS)

Revisado Por:
Denis Ricardo dos Santos
Diretor-Técnico Previdenciário do FPS
Matrícula nº 12976

A Política de Segurança da Informação, também referida como PSI, é o documento que orienta e estabelece as diretrizes do Fundo de Previdência Social – FPS, para a proteção dos ativos de informação e a prevenção de responsabilidade legal para todos os usuários. Deve, portanto, ser cumprida e aplicada em todas as áreas desta instituição.

A presente PSI está baseada nas recomendações propostas pela norma ABNT NBR ISO/IEC 27002:2013, reconhecida mundialmente como um código de prática para a gestão da segurança da informação, bem como está de acordo com as leis vigentes em nosso país.

OBJETIVOS

Estabelecer diretrizes que permitam aos servidores do FPS seguirem padrões de comportamento relacionados à segurança da informação adequados às necessidades da instituição e de proteção legal da instituição e do indivíduo.

Nortear a definição de normas e procedimentos específicos de segurança da informação, bem como a implementação de controles e processos para seu atendimento.

Preservar as informações do FPS quanto à:

• **Integridade:** garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais.

• **Confidencialidade:** garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.

• **Disponibilidade:** garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

APLICAÇÕES DA PSI

As diretrizes aqui estabelecidas deverão ser seguidas por todos os servidores deste Fundo de Previdência Social, bem como os prestadores de serviço, e se aplicam à informação em qualquer meio ou suporte.

Esta política dá ciência a cada servidor de que os ambientes, sistemas, computadores e redes da instituição poderão ser monitorados e gravados, com prévia informação, conforme previsto nas leis brasileiras.

É também obrigação de cada servidor manter-se atualizado em relação a esta PSI e aos procedimentos e normas relacionadas, buscando orientação do seu gestor ou da Área de TI sempre que não estiver absolutamente seguro quanto à aquisição, uso e/ou descarte de informações.

PRINCÍPIOS DA PSI

Toda informação produzida ou recebida pelos servidores e prestadores de serviços como resultado da atividade profissional contratada pelo FPS pertence à referida instituição. As exceções devem ser explícitas e formalizadas em contrato entre as partes.

Os equipamentos de informática e comunicação, sistemas e informações são utilizados pelos servidores para a realização das atividades profissionais. O uso

pessoal dos recursos é permitido desde que não prejudique o desempenho dos sistemas e serviços.

REQUISITOS DA PSI

Para a uniformidade da informação, a PSI deverá ser comunicada a todos os servidores do FPS a fim de que a política seja cumprida dentro e fora da instituição.

Deverá haver um comitê responsável pela gestão da segurança da informação, o qual foi designado como *Comitê de Segurança da Informação - Cosin*.

Tanto a PSI quanto as normas deverão ser revistas e atualizadas periodicamente, sempre que algum fato relevante ou evento motive sua revisão antecipada, conforme análise e decisão do *Cosin*.

Deverá constar em todos os contratos do FPS o anexo de Acordo de Confidencialidade ou Cláusula de Confidencialidade, como condição imprescindível para que possa ser concedido o acesso aos ativos de informação disponibilizados pela instituição.

A responsabilidade em relação à segurança da informação deve ser comunicada na fase de contratação dos servidores ou prestadores de serviços. Todos os servidores ou prestadores de serviço devem ser orientados sobre os procedimentos de segurança, bem como o uso correto dos ativos, a fim de reduzir possíveis riscos. Eles devem assinar um termo de responsabilidade.

Todo incidente que afete a segurança da informação deverá ser comunicado inicialmente à **Área de Tecnologia da Informação** (TI) deste FPS. Esse setor poderá encaminhar posteriormente ao Comitê de Segurança da Informação para análise, se julgar necessário.

Um plano de contingência e a continuidade dos principais sistemas e serviços deverão ser implantados e testados no mínimo anualmente, visando reduzir riscos de perda de confidencialidade, integridade e disponibilidade dos ativos de informação.

Todos os requisitos de segurança da informação, incluindo a necessidade de planos de contingência, devem ser identificados na fase de levantamento de escopo de um projeto ou sistema, e justificados, acordados, documentados, implantados e testados durante a fase de execução.

Deverão ser criados e instituídos controles apropriados, trilhas de auditoria ou registros de atividades, em todos os pontos e sistemas em que a instituição julgar necessário para reduzir os riscos dos seus ativos de informação como, por exemplo,

nas estações de trabalho, notebooks, nos acessos à internet, no correio eletrônico, nos sistemas contábeis e financeiros desenvolvidos pelo FPS ou por terceiros.

Os ambientes de produção devem ser segregados e rigidamente controlados, garantindo o isolamento necessário em relação aos ambientes de desenvolvimento, testes e homologação.

Esta PSI será implementada no FPS por meio de procedimentos específicos, obrigatórios para todos os servidores ou prestadores de serviços, independentemente do nível hierárquico ou função na instituição, bem como de vínculo empregatício ou prestação de serviço.

DAS RESPONSABILIDADES ESPECÍFICAS

1 - Dos Servidores e Prestadores de Serviços em Geral

Entende-se por servidor toda e qualquer pessoa física, contratada ou prestadora de serviço por intermédio de pessoa jurídica ou não, que exerça alguma atividade dentro ou fora da instituição.

2 - Dos Gestores de Pessoas e/ou Processos

Ter postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os servidores ou prestadores de serviços sob a sua gestão.

Atribuir aos servidores ou prestadores de serviços, na fase de contratação e de formalização dos contratos individuais de trabalho, de prestação de serviços ou de parceria, a responsabilidade do cumprimento da PSI do FPS.

Exigir dos servidores ou prestadores de serviços a assinatura do Termo de Compromisso e Ciência, assumindo o dever de seguir as normas estabelecidas, bem como se comprometendo a manter sigilo e confidencialidade, mesmo quando desligado, sobre todos os ativos de informações do FPS.

Antes de conceder acesso às informações da instituição, exigir a assinatura do Acordo de Confidencialidade dos servidores casuais e prestadores de serviços que não estejam cobertos por um contrato existente, por exemplo, durante a fase de levantamento para apresentação de propostas comerciais.

Adaptar as normas, os processos, procedimentos e sistemas sob sua responsabilidade para atender a esta PSI.

3 - Dos Custodiantes da Informação

3.1 - Da Área de Tecnologia da Informação (TI)

Testar a eficácia dos controles utilizados e informar aos gestores os riscos residuais.

Acordar com os gestores o nível de serviço que será prestado e os procedimentos de resposta aos incidentes.

Configurar os equipamentos, ferramentas e sistemas concedidos aos servidores com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos por esta PSI.

Os administradores e operadores dos sistemas computacionais podem, pela característica de seus privilégios como usuários, acessar os arquivos e dados de outros usuários. No entanto, isso só será permitido quando for necessário para a execução de atividades operacionais sob sua responsabilidade como, por exemplo, a manutenção de computadores, a realização de cópias de segurança, auditorias ou testes no ambiente.

Segregar as funções administrativas e operacionais a fim de restringir ao mínimo necessário os poderes de cada indivíduo e eliminar, ou ao menos reduzir, a existência de pessoas que possam excluir os logs e trilhas de auditoria das suas próprias ações.

Gerar e manter as trilhas para auditoria com nível de detalhe suficiente para rastrear possíveis falhas e fraudes. Para as trilhas geradas e/ou mantidas em meio eletrônico, implantar controles de integridade para torná-las juridicamente válidas como evidências.

Administrar, proteger e testar as cópias de segurança dos programas e dados relacionados aos processos críticos e relevantes para o FPS.

Implantar controles que gerem registros auditáveis para retirada e transporte de mídias das informações custodiadas pela área de TI, nos ambientes totalmente controlados por ela.

O gestor da área de TI deve ser previamente informado sobre o fim do prazo de retenção, para que tenha a alternativa de alterá-lo antes que a informação seja definitivamente descartada pelo custodiante.

Quando ocorrer movimentação interna dos ativos de TI, garantir que as informações de um usuário não serão removidas de forma irrecuperável antes de disponibilizar o ativo para outro usuário.

Planejar, implantar, fornecer e monitorar a capacidade de armazenagem, processamento e transmissão necessários para garantir a segurança requerida pelas áreas da instituição.

Atribuir cada conta ou dispositivo de acesso a computadores, sistemas, bases de dados e qualquer outro ativo de informação a um responsável identificável como pessoa física, sendo que:

- os usuários (logins) individuais de funcionários serão de responsabilidade do próprio funcionário.

- os usuários (logins) de terceiros serão de responsabilidade do gestor da área de TI.

Proteger continuamente todos os ativos de informação da instituição contra código malicioso, e garantir que todos os novos ativos só entrem para o ambiente de produção após estarem livres de código malicioso e/ou indesejado.

Garantir que não sejam introduzidas vulnerabilidades ou fragilidades no ambiente de produção da instituição em processos de mudança, sendo ideal a auditoria de código e a proteção contratual para controle e responsabilização no caso de uso de terceiros.

Definir as regras formais para instalação de software e hardware em ambiente de produção da instituição, exigindo o seu cumprimento dentro da instituição.

Realizar auditorias periódicas de configurações técnicas e análise de riscos.

Responsabilizar-se pelo uso, manuseio, guarda de assinatura e certificados digitais.

Garantir, da forma mais rápida possível, com solicitação formal, o bloqueio de acesso de usuários por motivo de desligamento da instituição, incidente, investigação ou outra situação que exija medida restritiva para fins de salvaguardar os ativos da instituição.

Monitorar o ambiente de TI, gerando indicadores e históricos de:

- uso da capacidade instalada da rede e dos equipamentos;
- tempo de resposta no acesso à internet e aos sistemas críticos do FPS;
- períodos de indisponibilidade no acesso à internet e aos sistemas críticos do FPS;
- incidentes de segurança (vírus, trojans, furtos, acessos indevidos, e assim por diante);

• atividade de todos os colaboradores durante os acessos às redes externas, inclusive internet (por exemplo: sites visitados, e-mails recebidos/enviados, upload/download de arquivos, entre outros);

4 - Da Área de Segurança da Informação

Propor as metodologias e os processos específicos para a segurança da informação, como avaliação de risco e sistema de classificação da informação.

Propor e apoiar iniciativas que visem à segurança dos ativos de informação do FPS.

Publicar e promover as versões da PSI e as Normas de Segurança da Informação aprovadas pelo Comitê de Segurança da Informação.

Promover a conscientização dos servidores e prestadores de serviços em relação à relevância da segurança da informação para FPS, mediante campanhas, palestras, treinamentos e outros meios de endomarketing.

Apoiar a avaliação e a adequação de controles específicos de segurança da informação para novos sistemas ou serviços.

Analisar criticamente incidentes em conjunto com o Comitê de Segurança da Informação.

Apresentar as atas e os resumos das reuniões do Comitê de Segurança da Informação, destacando os assuntos que exijam intervenção do próprio comitê ou do diretor-presidente da instituição.

Manter comunicação efetiva com o Comitê de Segurança da Informação sobre assuntos relacionados ao tema que afetem ou tenham potencial para afetar o bom andamento das atividades deste FPS.

4.1 - Do Comitê de Segurança da Informação

Deverá o CSI reunir-se formalmente pelo menos uma vez a cada seis meses. Reuniões adicionais devem ser realizadas sempre que for necessário deliberar sobre algum incidente grave ou definição relevante para o FPS.

O CSI poderá utilizar especialistas, internos ou externos, para apoiarem nos assuntos que exijam conhecimento técnico específico.

Cabe ao CSI:

• propor investimentos relacionados à segurança da informação com o objetivo de reduzir mais os riscos;
• propor alterações nas versões da PSI e a inclusão, a eliminação ou a mudança de normas complementares;
• avaliar os incidentes de segurança e propor ações corretivas;
• definir as medidas cabíveis nos casos de descumprimento da PSI e/ou das Normas de Segurança da Informação.

5 - DO MONITORAMENTO E DA AUDITORIA DO AMBIENTE

Para garantir as regras mencionadas nesta PSI o FPS poderá:

• implantar sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou wireless e outros componentes da rede – a informação gerada por esses sistemas poderá ser usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado;
• tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial, solicitação do diretor-presidente ou por determinação do Comitê de Segurança da Informação;
• realizar, a qualquer tempo, inspeção física nas máquinas de sua propriedade;
• instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso.

CORREIO ELETRÔNICO

O objetivo desta norma é informar aos colaboradores do FPS quais são as atividades permitidas e proibidas quanto ao uso do correio eletrônico da instituição. O uso do correio eletrônico do FPS é para fins da instituição e relacionados às atividades do servidor usuário dentro da instituição. A utilização desse serviço para fins pessoais é permitida desde que feita com bom senso, não prejudique o FPS e também não cause impacto no tráfego da rede.

Acrescentamos que é proibido aos servidores o uso do correio eletrônico do FPS:

• enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas a uso legítimo da instituição;
• enviar mensagem por correio eletrônico pelo endereço de seu departamento ou usando o nome de usuário de outra pessoa ou

endereço de correio eletrônico que não esteja autorizado a utilizar;
• enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou o FPS ou suas unidades vulneráveis a ações civis ou criminais;
• divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário desse ativo de informação;
• falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários, com o objetivo de evitar as punições previstas;
• apagar mensagens pertinentes de correio eletrônico quando qualquer estiver sujeita a algum tipo de investigação.
• produzir, transmitir ou divulgar mensagem que:

- contenha qualquer ato ou forneça orientação que conflite ou contrarie os interesses do FPS;
- contenha ameaças eletrônicas, como: spam, mail bombing, vírus de computador;
- contenha arquivos com código executável (.exe, .com, .bat, .pif, .js, .vbs, .hta, .src, .cpl, .reg, .dll, .inf) ou qualquer outra extensão que represente um risco à segurança;
- vise obter acesso não autorizado a outro computador, servidor ou rede;
- vise interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
- vise burlar qualquer sistema de segurança;
- vise vigiar secretamente ou assediar outro usuário;
- vise acessar informações confidenciais sem explícita autorização do proprietário;
- vise acessar indevidamente informações que possam causar prejuízos a qualquer pessoa;
- inclua imagens criptografadas ou de qualquer forma mascaradas;
- contenha anexo(s) superior(es) a 15 MB para envio (interno e internet) e 15 MB para recebimento (internet);
- tenha conteúdo considerado impróprio, obsceno ou ilegal;
- seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico entre outros;
- contenha perseguição preconceituosa baseada em sexo, raça, incapacidade física ou mental ou outras situações protegidas;
- tenha fins políticos locais ou do país (propaganda política);

 inclua material protegido por direitos autorais sem a permissão do detentor dos direitos.

As mensagens de correio eletrônico sempre deverão incluir assinatura conforme o modelo a ser criado e disponibilizado.

INTERNET

Todas as regras atuais do FPS visam basicamente o desenvolvimento de um comportamento eminentemente ético e profissional do uso da internet. Embora a conexão direta e permanente da rede da instituição com a internet ofereça um grande potencial de benefícios, ela abre a porta para riscos significativos para os ativos de informação.

Qualquer informação que é acessada, transmitida, recebida ou produzida na internet está sujeita a divulgação e auditoria. Portanto, o FPS, em total conformidade legal, reserva-se o direito de monitorar e registrar todos os acessos a ela.

Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet são de propriedade da instituição, que pode analisar e, se necessário, bloquear qualquer arquivo, site, correio eletrônico, domínio ou aplicação armazenados na rede/internet, estejam eles em disco local, na estação ou em áreas privadas da rede, visando assegurar o cumprimento de sua Política de Segurança da Informação.

O FPS, ao monitorar a rede interna, pretende garantir a integridade dos dados e programas. Toda tentativa de alteração dos parâmetros de segurança, por qualquer servidor ou prestador de serviço, sem o devido credenciamento e a autorização para tal, será julgada inadequada e os riscos relacionados serão informados ao servidor e ao respectivo gestor. O uso de qualquer recurso para atividades ilícitas poderá acarretar as ações administrativas e as penalidades decorrentes de processos civil e criminal, sendo que nesses casos a instituição cooperará ativamente com as autoridades competentes.

A internet disponibilizada pela instituição aos seus servidores, independentemente de sua relação contratual, pode ser utilizada para fins pessoais, desde que não prejudique o andamento dos trabalhos na instituição.

Como é do interesse do FPS que seus servidores e prestadores de serviços estejam bem informados, o uso de sites de notícias ou de serviços, por exemplo, é aceitável, desde que não comprometa a banda da rede em horários estritamente comerciais, não perturbe o bom andamento dos trabalhos nem implique conflitos de interesse com os objetivos da instituição.

Somente os servidores que estão devidamente autorizados a falar em nome do FPS para os meios de comunicação poderão manifestar-se, seja por e-mail, entrevista on-line, podcast, seja por documento físico, entre outros.

Apenas os servidores e prestadores de serviços autorizados pela instituição poderão copiar, captar, imprimir ou enviar imagens da tela para terceiros, devendo atender à norma interna de uso de imagens, à Lei de Direitos Autorais, à proteção da imagem garantida pela Constituição Federal e demais dispositivos legais.

É proibida a divulgação e/ou o compartilhamento indevido de informações da área administrativa em listas de discussão, sites ou comunidades de relacionamento, salas de batepapo ou chat, comunicadores instantâneos ou qualquer outra tecnologia correlata que venha surgir na internet.

Os servidores com acesso à internet poderão fazer o download (baixa) somente de programas ligados diretamente às suas atividades no FPS e deverão providenciar o que for necessário para regularizar a licença e o registro desses programas, desde que autorizados pela área de TI ou comitê de segurança da informação.

O uso, a instalação, a cópia ou a distribuição não autorizada de softwares que tenham direitos autorais, marca registrada ou patente na internet são expressamente proibidos. Qualquer software não autorizado baixado será excluído pela área de TI.

Os servidores e prestadores de serviços não poderão em hipótese alguma utilizar os recursos do FPS para fazer o download ou distribuição de software ou dados pirateados, atividade considerada delituosa de acordo com a legislação nacional.

Como regra geral, materiais de cunho sexual não poderão ser expostos, armazenados, distribuídos, editados, impressos ou gravados por meio de qualquer recurso.

Servidores ou Prestadores de Serviços com acesso à internet não poderão efetuar upload (subida) de qualquer software licenciado ao FPS ou de dados de sua propriedade, sem expressa autorização do responsável pelo software ou pelos dados.

Os colaboradores não poderão utilizar os recursos do FPS para deliberadamente propagar qualquer tipo de vírus, worm, cavalo de troia, spam, assédio, perturbação ou programas de controle de outros computadores.

O acesso a softwares como aqueles relacionados a compartilhamento de arquivos (Ex.: eMule, uTorrent, BitTorrent), troca de mensagens em tempo real (Ex.: Facebook, Instagram para PC), transmissão de áudio e vídeo (Ex.: TapinRadio,

Google Play), telefonia Internet (Ex.: Skype), não serão permitidos, evitando assim que a segurança e o desempenho da rede institucional sejam afetados.

IDENTIFICAÇÃO

Os dispositivos de identificação e senhas protegem a identidade do servidor usuário, evitando e prevenindo que uma pessoa se faça passar por outra perante o FPS e/ou terceiros.

O uso dos dispositivos e/ou senhas de identificação de outra pessoa constitui crime tipificado no Código Penal Brasileiro (art. 307 – falsa identidade).

Tal norma visa estabelecer critérios de responsabilidade sobre o uso dos dispositivos de identificação e deverá ser aplicada a todos os colaboradores.

Todo e qualquer dispositivo de identificação pessoal, portanto, não poderá ser compartilhado com outras pessoas em nenhuma hipótese.

Se existir login de uso compartilhado por mais de um servidor, a responsabilidade perante o FPS e a legislação (cível e criminal) será dos usuários que dele se utilizarem. Somente se for identificado conhecimento ou solicitação do gestor de uso compartilhado ele deverá ser responsabilizado.

É proibido o compartilhamento de login para funções de administração de sistemas.

A Área de TI responde pela criação da identidade lógica dos servidores na instituição, nos termos do Procedimento para Gerenciamento de Contas de Grupos e Usuários.

Devem ser distintamente identificados os visitantes, estagiários, empregados temporários, empregados regulares e prestadores de serviços, sejam eles pessoas físicas e/ou jurídicas. Ao realizar o primeiro acesso ao ambiente de rede local, o usuário deverá trocar imediatamente a sua senha conforme as orientações apresentadas.

Os usuários que não possuem perfil de administrador deverão ter senha de tamanho variável, possuindo no mínimo 6 (seis) caracteres alfanuméricos, utilizando caracteres especiais (@ # $ %) e variação entre caixa-alta e caixa-baixa (maiúsculo e minúsculo) sempre que possível.

Já os usuários que possuem perfil de administrador ou acesso privilegiado deverão utilizar uma senha de no mínimo 10 (dez) caracteres, alfanumérica, utilizando caracteres especiais (@ # $ %) e variação de caixa-alta e caixa-baixa (maiúsculo e minúsculo) obrigatoriamente.

É de responsabilidade de cada usuário a memorização de sua própria senha, bem como a proteção e a guarda dos dispositivos de identificação que lhe forem designados.

As senhas não devem ser anotadas ou armazenadas em arquivos eletrônicos (Word, Excel, etc.), compreensíveis por linguagem humana (não criptografados); não devem ser baseadas em informações pessoais, como próprio nome, nome de familiares, data de nascimento, endereço, placa de veículo, nome da empresa, nome do departamento; e não devem ser constituídas de combinações óbvias de teclado, como “abcdefgh”, “87654321”, entre outras.

Após 3 (três) tentativas de acesso, a conta do usuário será bloqueada. Para o desbloqueio é necessário que o usuário entre em contato com a área de TI do FPS. Deverá ser estabelecido um processo para a renovação de senha (confirmar a identidade).

Os usuários podem alterar a própria senha, e devem ser orientados a fazê-lo, caso suspeitem que terceiros obtiveram acesso indevido ao seu login/senha.

A periodicidade máxima para troca das senhas é 45 (quarenta e cinco) dias, não podendo ser repetidas as 3 (três) últimas senhas. Os sistemas críticos e sensíveis para a instituição e os logins com privilégios administrativos devem exigir a troca de senhas a cada 30 dias. Os sistemas devem forçar a troca das senhas dentro desse prazo máximo.

Todos os acessos devem ser imediatamente bloqueados quando se tornarem desnecessários. Portanto, assim que algum usuário for demitido ou solicitar demissão, o Departamento de Recursos Humanos deverá imediatamente comunicar tal fato a área de TI, a fim de que essa providência seja tomada. A mesma conduta se aplica aos usuários cujo contrato ou prestação de serviços tenha se encerrado, bem como aos usuários de testes e outras situações similares.

Caso o servidor esqueça sua senha, ele deverá requisitar formalmente a troca ou comparecer pessoalmente à área de TI responsável para cadastrar uma nova.

COMPUTADORES E RECURSOS TECNOLÓGICOS

Os equipamentos disponíveis aos servidores são de propriedade do FPS, cabendo a cada um utilizá-los e manuseá-los corretamente para as atividades de interesse da instituição, bem como cumprir as recomendações constantes nos procedimentos operacionais fornecidos pelas gerências responsáveis.

É proibido todo procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação, sem o conhecimento prévio e o

acompanhamento de um servidor da área de TI, ou de quem este determinar. As áreas que necessitarem fazer testes deverão solicitá-los previamente à área de TI, ficando responsáveis jurídica e tecnicamente pelas ações realizadas.

Todas as atualizações e correções de segurança do sistema operacional ou aplicativos somente poderão ser feitas após a devida validação no respectivo ambiente de homologação, e depois de sua disponibilização pelo fabricante ou fornecedor.

Os sistemas e computadores devem ter versões do software antivírus instaladas, ativadas e atualizadas permanentemente. O usuário, em caso de suspeita de vírus ou problemas na funcionalidade, deverá acionar área de TI.

A transferência e/ou a divulgação de qualquer software, programa ou instruções de computador para terceiros, por qualquer meio de transporte (físico ou lógico), somente poderá ser realizada com a devida identificação do solicitante, se verificada positivamente e estiver de acordo com a classificação de tal informação e com a real necessidade do destinatário.

Arquivos pessoais e/ou não pertinentes a instituição (fotos, músicas, vídeos, etc) não deverão ser copiados/movidos para os drives de rede, pois podem sobrecarregar o armazenamento nos servidores. Caso identificada a existência desses arquivos, eles poderão ser excluídos definitivamente por meio de comunicação prévia ao usuário.

Documentos imprescindíveis para as atividades dos servidores da instituição deverão ser salvos em drives de rede. Tais arquivos, se gravados apenas localmente nos computadores (por exemplo, no drive C:), não terão garantia de backup e poderão ser perdidos caso ocorra uma falha no computador, sendo, portanto, de responsabilidade do próprio usuário.

Os servidores do FPS e/ou detentores de contas privilegiadas não devem executar nenhum tipo de comando ou programa que venha sobrecarregar os serviços existentes na rede da instituição sem a prévia solicitação e a autorização da área de TI.

No uso dos computadores, equipamentos e recursos de informática, algumas regras devem ser atendidas:

- Os servidores devem informar a área de TI qualquer identificação de dispositivo estranho conectado ao seu computador;
- É vedada a abertura ou o manuseio de computadores ou outros equipamentos de informática para qualquer tipo de reparo que não seja realizado por um servidor da área de TI do FPS ou por terceiros devidamente contratados para o serviço;

• Todos os modems internos ou externos devem ser removidos ou desativados para impedir a invasão/evasão de informações, programas, vírus. Em alguns casos especiais, conforme regra específica, será considerada a possibilidade de uso para planos de contingência mediante a autorização da área de TI;
• É expressamente proibido o consumo de alimentos, bebidas ou fumo na mesa de trabalho e próximo aos equipamentos;
• O servidor deverá manter a configuração do equipamento disponibilizado pelo FPS, seguindo os devidos controles de segurança exigidos pela Política de Segurança da Informação, assumindo a responsabilidade como custodiante de informações;
• Deverão ser protegidos por senha (bloqueados), nos termos previstos pela Norma de Autenticação, todos os terminais de computador e impressoras quando não estiverem sendo utilizados;
• Todos os recursos tecnológicos adquiridos pelo FPS devem ter imediatamente suas senhas padrões (default) alteradas;
• Os equipamentos deverão manter preservados, de modo seguro, os registros de eventos, constando identificação dos servidores, datas e horários de acesso.

Acrescentamos algumas situações em que é proibido o uso de computadores e recursos tecnológicos do FPS.

• Tentar ou obter acesso não autorizado a outro computador, servidor ou rede;
• Burlar quaisquer sistemas de segurança;
• Acessar informações confidenciais sem explícita autorização do proprietário;
• Vigiar secretamente outrem por dispositivos eletrônicos ou softwares, como, por exemplo, analisadores de pacotes (sniffers);
• Interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
• Usar qualquer tipo de recurso tecnológico para cometer ou ser cúmplice de atos de violação, assédio sexual, perturbação, manipulação ou supressão de direitos autorais ou propriedades intelectuais sem a devida autorização legal do titular;
• Hospedar pornografia, material racista ou qualquer outro que viole a legislação em vigor no país, a moral, os bons costumes e a ordem pública;
• Utilizar software pirata, atividade considerada delituosa de acordo com a legislação nacional.

BACKUP

Todos os procedimentos de backup devem ser automatizados por sistemas de agendamento automatizado para que sejam preferencialmente executados fora do horário comercial, nas chamadas “janelas de backup” – períodos em que não há nenhum ou pouco acesso de usuários ou processos automatizados aos sistemas de informática.

Os servidores responsáveis pela gestão dos sistemas de backup deverão realizar pesquisas frequentes para identificar atualizações de correção, novas versões do produto, ciclo de vida (quando o software não terá mais garantia do fabricante), sugestões de melhorias, entre outros.

As mídias de backup (como Disco HD, e outros) devem ser acondicionadas em local seco, climatizado, seguro (de preferência em cofres corta-fogo segundo as normas da ABNT) e distantes o máximo possível do FPS.

É necessária a previsão, em orçamento anual, da renovação das mídias em razão de seu esgotamento, bem como deverá ser mantido um estoque constante das mídias para qualquer uso emergencial.

Quaisquer atrasos na execução de backup ou restore deverão ser justificados formalmente pelos responsáveis pelos Backups.

Testes de restauração (restore) de backup devem ser executados por seus responsáveis, nos termos dos procedimentos específicos, aproximadamente a cada 30 ou 60 dias, de acordo com a criticidade do backup.

Por se tratar de uma simulação, o executor deve restaurar os arquivos em local diferente do original, para que assim não sobreponha os arquivos válidos.

DAS DISPOSIÇÕES FINAIS

Assim como a ética, a política de segurança da informação (PSI) deve ser entendida como parte fundamental da cultura interna do Fundo de Previdência Social.

A PSI trata-se do conjunto de ações, de técnicas e de boas práticas relacionadas ao uso seguro de informações, o que garante que os dados sejam protegidos, de pessoas não autorizadas.

Além disto, serve para administrar corretamente eventuais ocorrências e emergências, diante dos quais, com um plano de contingência, é possível saber como agir para prevenir danos maiores aos dados.

Assim, a segurança da informação se baseia em três pilares: confiabilidade, integridade e disponibilidade. O primeiro determina que os dados só podem ser acessados por pessoas autorizadas, enquanto o segundo dispõe que somente quem tiver a permissão pode modificar as informações, e o terceiro estabelece que as informações precisam estar sempre disponíveis para os autorizados, conforme a solicitação.

Para completar, a Política de Segurança da informação tem como seu princípio fundamental propiciar e garantir um ambiente seguro onde todas as atividades deste Fundo de Previdência Social sejam realizadas com êxito e segurança.