Política de Segurança da Informação

V.2 em 08/2021

Índice

1. DEFINIÇÕES

- **ACESSO LÓGICO**: acesso a rede de computadores, sistemas e estações de trabalho por meio de autenticação;

- **ACESSO REMOTO:** ingresso, por meio de uma rede, aos dados de um computador fisicamente distante da máquina do usuário;

- **AGENTE RESPONSÁVEL**: Servidor Público ocupante de cargo efetivo de carreira ou comissionado na Taboãoprev, direta ou indiretamente incumbido de chefiar e gerenciar os funcionários da Taboãoprev que sejam usuários, produtores e/ou manipuladores das informações no âmbito da autarquia;

- **ADSL (ASYMMETRIC DIGITAL SUBSCRIBER LINE) LINHA DIGITAL ASSIMÉTRICA PARA ASSINANTE**: tecnologia de transmissão que possibilita o transporte de voz e dados a alta velocidade através da rede telefônica convencional, analógica ou digital;

- **AMEAÇA**: conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um arquivo, sistema ou para a autarquia;

- **ANÁLISE/AVALIAÇÃO DE RISCOS**: processo completo de análise e avaliação de riscos;

- **ATIVO**: qualquer bem, tangível ou intangível, que a autarquia possua e que tenha valor para a organização;

- **ATIVO DA INFORMAÇÃO**: os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles tem acesso;

- **ATIVO SIGILOSO**: qualquer bem tangível ou intangível que possa conter informações sigilosas que, se acessadas por pessoas não autorizadas, podem causar danos significativos à Taboãoprev e seus segurados;

- **AUDITORIA**: verificação e avaliação dos sistemas e procedimentos internos com o objetivo de reduzir e/ou eliminar fraudes, erros, práticas ineficientes ou ineficazes;

- **AUTENTICAÇÃO**: é o ato de confirmar que algo ou alguém é autêntico, ou seja, uma garantia de que qualquer alegação de ou sobre um objeto é verdadeira;

- **AUTENTICIDADE**: a certeza de que um objeto ou informação provém das fontes anunciadas e que não foi alvo de mutações ao longo do processo. Identificação e segurança da origem da informação. Garantia de que você é quem diz ser;

- **BANCO DE DADOS (OU BASE DE DADOS)**: é um sistema de armazenamento de dados, ou seja, um conjunto de registros que tem como objetivo organizar e guardar as informações;

- **BLOQUEIO DE ACESSO**: processo que tem por finalidade suspender temporariamente o acesso;

- **BLUETOOTH**: tecnologia de transmissão de dados via sinais de rádio de alta frequência, entre dispositivos eletrônicos próximos;

- **CLASSIFICAÇÃO DA INFORMAÇÃO**: atribuição, pela autoridade competente, de grau de sigilo dado à informação, documento, material, área ou instalação;

- **CONFIDENCIALIDADE**: propriedade de que a informação não esteja disponível ou revelada a pessoa física ou jurídica, sistema, órgão ou entidade não autorizado e credenciado;

- **CONTROLE DE ACESSO:** conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso;

- **CÓPIA DE SEGURANÇA (BACKUP):** copiar dados em um meio separado do original, de forma a protegê-los de qualquer eventualidade. Essencial para dados importantes;

- **CORREIO ELETRÔNICO:** é um método que permite compor, enviar e receber mensagens através de sistemas eletrônicos de comunicação;

- **CREDENCIAIS OU CONTAS DE ACESSO:** permissões, concedidas por autoridade competente após o processo de credenciamento, que habilitam determinada pessoa, sistema ou organização ao acesso. A credencial pode ser física como crachá, cartão e selo ou lógica como identificação de usuário e senha;

- **CRIPTOGRAFIA:** é o estudo dos princípios e técnicas pelas quais a informação pode ser transformada da sua forma original para outra ilegível, de forma que possa ser conhecida apenas por seu destinatário (detentor da "chave secreta");

- **DADO:** representação de uma informação, instrução, ou conceito, de modo que possa ser armazenado e processado por um computador;

- **DIRETRIZ:** descrição que orienta o que deve ser feito, e como, para se alcançar os objetivos estabelecidos nas políticas;

- **DISPONIBILIDADE:** propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade;

- **DOWNLOAD - (BAIXAR):** copiar arquivos de um servidor (site) na internet para um computador pessoal;

- **ESPELHAMENTO:** Sistema de proteção de dados onde o conteúdo é espelhado em tempo real. Todos os dados são duplicados entre as áreas de armazenamento disponíveis.

- **EQUIPE DE TRATAMENTO E RESPOSTA A INCIDENTES EM REDES COMPUTACIONAIS (ETIR):** grupo de pessoas com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores;

- **FTP (FILE TRANSFER PROTOCOL) - PROTOCOLO DE TRANSFERÊNCIA DE ARQUIVO:** é um protocolo da Internet para transferência de arquivos;

- **GESTÃO DE CONTINUIDADE DE NEGÓCIOS:** Processo de gestão global que identifica as potenciais ameaças para uma organização e os impactos nas operações da instituição que essas ameaças, se concretizando, poderiam causar, e fornecendo e mantendo um nível aceitável de serviço face a rupturas e desafios à operação normal do dia-a-dia;

- **GESTÃO DE RISCO:** conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos;

- **GESTÃO DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES:** conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos;

- **GESTOR DA INFORMAÇÃO:** pessoa responsável pela administração de informações geradas em seu processo de trabalho e/ou sistemas de informação relacionados às suas atividades;

- **GESTOR DE SEGURANÇA DA INFORMAÇÃO E DAS COMUNICAÇÕES:** é responsável pelas ações de segurança da informação e comunicações no âmbito do órgão ou entidade da APF;

- **HARDWARE:** É a parte física do computador, conjunto de componentes eletrônicos, circuitos integrados e periféricos, como a máquina em si, placas, impressora, teclado e outros;

- **HTTP (HYPER TEXT TRANSFER PROTOCOL) - PROTOCOLO DE TRANSFERÊNCIA DE HIPERTEXTO:** é uma linguagem para troca de informação entre servidores e clientes da rede;

- **HTTPS (HYPERTEXT TRANSFER PROTOCOL SECURE) – PROTOCOLO DE TRANSFERÊNCIA DE HIPERTEXTO SEGURO:** é uma linguagem para troca de informação entre servidores e clientes da rede, com recursos de criptografia, autenticação e integridade;

- **INCIDENTE DE SEGURANÇA:** é qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

- **INFORMAÇÃO:** dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

- **INFORMAÇÕES CRÍTICAS:** são as informações de extrema importância para a sobrevivência da instituição;

- **INFORMAÇÃO SIGILOSA:** informação submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado, e aquelas abrangidas pelas demais hipóteses legais de sigilo;

- **INSTANT MESSENGER – MENSAGEIRO INSTANTÂNEO:** é uma aplicação que permite o envio e o recebimento de mensagens em tempo real;

- **INTEGRIDADE:** propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

- **INTERNET:** rede mundial de computadores;

- **INTERNET PROTOCOL – PROTOCOLO DE INTERNET:** é um protocolo de comunicação usado entre duas ou mais máquinas em rede para encaminhamento dos dados;

- **INTRANET:** rede de computadores privada que faz uso dos mesmos protocolos da Internet. Pode ser entendida como rede interna de alguma instituição em que geralmente o acesso ao seu conteúdo é restrito;

- **LOG:** é o termo utilizado para descrever o processo de registro de eventos relevantes num sistema computacional. Esse registro pode ser utilizado para reestabelecer o estado original de um sistema ou para que um administrador conheça o seu comportamento no passado. Um arquivo de log pode ser utilizado para auditoria e diagnóstico de problemas em sistemas computacionais;

- **LOGON:** Procedimento de identificação e autenticação do usuário nos Recursos de Tecnologia da Informação. É pessoal e intransferível;

- **ON LINE – ESTAR DISPONÍVEL AO VIVO:** no contexto da Internet significa estar disponível para acesso imediato, em tempo real;

- **PERFIL DE ACESSO:** conjunto de atributos de cada usuário, definidos previamente como necessários para credencial de acesso;

- **PLANO DE CONTINGÊNCIA:** Descrever as medidas a serem tomadas por uma empresa, incluindo a ativação de processos manuais, para fazer com que seus processos críticos voltem a funcionar plenamente, ou num estado minimamente aceitável, o mais rápido possível, evitando assim uma paralisação prolongada;

- **PEER-TO-PEER (P2P) – PONTO A PONTO:** permite conectar o computador de um usuário a outro, para compartilhar ou transferir dados, como MP3, vídeos, imagens, entre outros;

- **POLÍTICA DE SEGURANÇA DA INFORMAÇÃO:** documento aprovado pela autoridade responsável pelo órgão ou entidade da Administração Pública Federal, direta e indireta, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação;

- **PROTOCOLO:** convenção ou padrão que controla e possibilita uma conexão, comunicação, transferência de dados entre dois sistemas computacionais. Método padrão que permite a comunicação entre processos, conjunto de regras e procedimentos para emitir e receber dados numa rede;

- **PROXY:** é um serviço intermediário entre as estações de trabalho de uma rede e a Internet. O servidor de rede proxy serve para compartilhar a conexão com a Internet, melhorar o desempenho do acesso, bloquear acesso a determinadas páginas;

- **QUEBRA DE SEGURANÇA**: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e das comunicações;

- **RECURSOS COMPUTACIONAIS:** recursos que processam, armazenam e/ou transmitem informações, tais como aplicações, sistemas de informação, estações de trabalho, notebooks, servidores de rede, equipamentos de conectividade e infraestrutura;

- **REDE CORPORATIVA:** conjunto de todas as redes locais sob a gestão da instituição;

- **REDE PÚBLICA:** rede de acesso a todos;

- **REPLICAÇÃO:** é a manutenção de cópias idênticas de dados em locais diferentes. O objetivo de um mecanismo de replicação de dados é permitir a manutenção de várias cópias idênticas de um mesmo dado em vários sistemas de armazenamento;

- **ROTEADOR:** equipamento responsável pela troca de informações entre redes;

- **SEGURANÇA DA INFORMAÇÃO:** ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

- **SERVIDOR DE REDE:** recurso de TI com a finalidade de disponibilizar ou gerenciar serviços ou sistemas informáticos;

- **SERVIDOR:** pessoa legalmente investida em cargo público;

- **SISTEMAS DE INFORMAÇÃO:** conjunto de meios de comunicação, computadores e redes de computadores, assim como dados e informações que podem ser armazenados, processados, recuperados ou transmitidos por serviços de telecomunicações, inclusive aplicativos, especificações e procedimentos para sua operação, uso e manutenção;

- **SISTEMA DE SEGURANÇA DA INFORMAÇÃO:** proteção de um conjunto de dados, no sentido de preservar o valor que possuem para um indivíduo ou uma organização. São características básicas da segurança da informação os atributos de confidencialidade, integridade, disponibilidade e autenticidade, não estando esta segurança restrita somente a sistemas computacionais, informações eletrônicas ou sistemas de armazenamento;

- **SOFTWARE:** são todos os programas existentes em um computador, como sistema operacional, aplicativos, entre outros;

- **SITE:** Conjunto de páginas virtuais dinâmicas ou estáticas, que tem como principal objetivo fazer a divulgação da instituição;

- **STREAMING:** transferência de dados (normalmente áudio e vídeo) em fluxo contínuo por meio da Internet;

- **SWITCHES:** Um switch de rede é um equipamento eletrônico de comutação que funciona como um nó central numa rede no formato estrela, armazenando em memória o endereço físico de todos os computadores conectados a ele, relacionando cada endereço físico a uma de suas portas e permitindo assim a interligação entre os dispositivos conectados;

- **TERMO DE RESPONSABILIDADE:** termo assinado pelo usuário concordando em contribuir com a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações que tiver acesso, bem como assumir responsabilidades decorrentes de tal acesso;

- **TRATAMENTO DA INFORMAÇÃO:** recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação, inclusive as sigilosas;

- **TRATAMENTO DE INCIDENTES DE SEGURANÇA EM REDES COMPUTACIONAIS:** serviço que consiste em receber, filtrar, classificar e responder às solicitações e alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências;

- **USUÁRIO:** servidores, terceirizados, colaboradores, consultores, auditores e estagiários que obtiveram autorização do responsável pela área interessada para acesso aos Ativos de Informação de um órgão ou entidade da APF, formalizada por meio da assinatura do Termo de Responsabilidade;

- **VLAN (VIRTUAL LOCAL AREA NETWORK OU VIRTUAL LAN) – REDE LOCAL VIRTUAL:** é um agrupamento lógico de estações, serviços e dispositivos de rede que não estão restritos a um segmento físico de uma rede local;

- **VPN (VIRTUAL PRIVATE NETWORK) – REDE PRIVADA VIRTUAL:** é uma rede de dados privada que faz uso das infraestruturas públicas de telecomunicações, preservando a privacidade, logo é a extensão de uma rede privada que engloba conexões com redes compartilhadas ou públicas. Com uma VPN pode-se enviar dados entre dois computadores através de uma rede compartilhada ou pública de uma maneira que emula uma conexão ponto a ponto privada;

- **VULNERABILIDADE:** conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou organização, os quais podem ser evitados por uma ação interna de segurança da informação;

- **WIRELESS - REDE SEM FIO:** rede que permite a conexão entre computadores e outros dispositivos através da transmissão e recepção de sinais de rádio.

2. REFERÊNCIAS LEGAIS E NORMATIVAS

- Lei 12527, de 18 de novembro de 2011 – Lei de acesso a informação;
- Lei nº 9.983, de 14 de julho de 2000: Altera o Decreto Lei nº 2848/40 – Código Penal, sobre tipificação de crimes por computador contra a Previdência Social e a Administração Pública;
- Lei n° 9.610, de 19 de fevereiro de 1998, que altera, atualiza e consolida a legislação sobre direitos autorais;
- Lei nº 8.159, de 08 de janeiro de 1991, dispõe sobre a política nacional de arquivos públicos e privados e dá outras providências e alterações legais;
- Código Civil, Art. 1.016, que institui que os administradores respondem solidariamente perante a sociedade e os terceiros prejudicados, por culpa no desempenho de suas funções;
- Cartilha de Segurança para Internet, desenvolvida pelo CERT.br, mantido pelo NIC.br, com inteiro teor em http://cartilha.cert.br/;

3. PRINCÍPIOS

São princípios de Segurança da Informação da Taboãoprev:

3.1 A garantia ao direito pessoal e coletivo à intimidade e ao sigilo da correspondência e das comunicações individuais; e

3.2 A proteção dos dados, informações e conhecimentos produzidos na Taboãoprev.

4. DIRETRIZES GERAIS

São diretrizes gerais de Segurança da Informação da Taboãoprev:

4.1 A preservação da disponibilidade, integridade, confiabilidade e autenticidade dos dados, informações e conhecimentos que compõem o ativo da informação da Taboãoprev;

4.2 Continuidade das atividades;

4.3 Economicidade da proteção dos ativos de informação;

4.4 Pessoalidade e utilidade do acesso aos ativos de informação;

4.5 A responsabilização do usuário pelos atos que comprometam a segurança do sistema da informação.

5. ORGANIZAÇÃO DA SEGURANÇA DA INFORMAÇÃO

5.1 A Política de Segurança da Informação é o instrumento que regula a proteção dos dados, informações e conhecimentos da instituição, com vistas à garantia de integridade, disponibilidade, conformidade e confiabilidade;

5.2 Todos os mecanismos de proteção utilizados para a segurança da informação devem ser mantidos para preservar a continuidade do negócio (regular exercício das funções institucionais);

5.3 O gerenciamento dos ativos de informação deverão observar normas operacionais e procedimentos específicos, a fim de garantir sua operação segura e contínua;

5.4 As medidas de proteção devem ser planejadas e os gastos da aplicação de controles devem ser compatíveis como valor do ativo protegido;

5.5 O acesso às informações, sistemas e instalações depende da apresentação de identificador único, pessoal, intransferível e com validade estabelecida, que permita de maneira clara e indiscutível o seu reconhecimento.

5.6 Todos os servidores e estagiários da Taboãoprev devem assinar uma "Declaração de Ciência e Compromisso a Política de Segurança da Informação – PSI", onde se comprometa em sua observância e acatamento.

6. SEGURANÇA EM RECURSOS HUMANOS

6.1 Todos os usuários devem ser conscientizados e treinados nos procedimentos de segurança da informação;

6.2 O controle operacional de uma atividade crítica não pode ser atribuição exclusiva de uma única pessoa;

6.3 Quando do afastamento, mudança de responsabilidades ou atribuições dentro da organização faz se necessária a revisão imediata dos direitos de acesso e uso dos ativos;

6.4 Quando da efetivação do desligamento de usuário, deverão ser extintos todos os direitos de acesso e uso dos ativos a ele atribuído.

7. COMPETÊNCIAS E RESPONSABILDADES

7.1 Essa Política e os procedimentos de segurança se aplicam a todos os servidores e estagiários da Taboãoprev.

8. COMPETE A DIRETORIA EXECUTIVA DA TABOÃOPREV

8.1 Promover cultura de segurança da informação e comunicações;

8.2 Acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;

8.3 Propor recursos necessários às ações de segurança da informação e comunicações;

8.4 Realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na segurança da informação e comunicações;

8.5 Propor normas relativas à segurança da informação e comunicações;

8.6 Editar Normas Complementares e Procedimentos de Segurança da Informação e das Comunicações;

8.7 Planejar e coordenar a execução dos programas, planos, projetos e ações de segurança;

8.8 Apurar os incidentes de segurança críticos e encaminhar os fatos apurados para aplicação das penalidades previstas;

8.9 Supervisionar, analisar e avaliar a efetividade dos processos, procedimentos, sistemas e dispositivos de segurança da informação;

8.10 Manter a análise de risco atualizada, refletindo o estado corrente da organização;

8.11 Identificar controles físicos, administrativos e tecnológicos para mitigação do risco;

8.12 Recepcionar, organizar, armazenar e tratar adequadamente as informações de eventos e incidentes de segurança, determinando aos respectivos gestores as ações corretivas ou contingentes em cada caso.

9. PENALIDADES

9.1 O não cumprimento das determinações da PSI sujeita o infrator às penalidades previstas na **Lei Complementar nº 224 de 16/08/2010 – Código Disciplinar dos Servidores Públicos Vinculados a Administração Pública Direta, Autárquica e Fundacional do Município de Taboão da Serra** e legislação complementar, bem como, nos regulamentos internos da Taboãoprev;

9.2 O descumprimento das disposições constantes nessa Política e nas Normas Complementares sobre segurança da informação caracteriza infração funcional, a ser apurada em processo administrativos disciplinar, sem prejuízo das responsabilidades penal e civil;

9.3 O usuário que fizer uso de forma indevida ou não autorizada dos recursos de tecnologia da informação, bem como agir em desacordo com os termos dessa política, fica sujeito à aplicação das penalidades previstas na legislação vigente;

9.4 Essa PSI deve ser revisada e atualizada anualmente, caso não ocorram eventos ou fatos relevantes que exijam uma revisão imediata.

10. VIGÊNCIA

10.1 Esta política foi aprovada pelos membros do Conselho Municipal de Previdência em decisão lavrada na Ata da 105ª Reunião Ordinária do CMP, foi revisada e atualizada em agosto de 2021, tendo sido aprovada e homologada pelo Conselho Municipal de Previdência na Ata da 165ª Reunião Ordinária.

10.2 Esse documento entra em vigor na data de sua publicação.

11. DISPOSIÇÕES FINAIS

11.1 Os casos omissos e as dúvidas com relação a essa PSI serão submetidos ao Conselho Municipal de Previdência.

A presente Política de Segurança da Informação – PSI foi revisada e reformulada em agosto de 2021. Foi devidamente apresentada aos conselheiros, tendo sido aprovada e homologada pelo Conselho Municipal de Previdência na Ata da 165ª Reunião Ordinária, Conselho Fiscal na Ata da 124ª Reunião Ordinária e Comitê de Investimentos na Ata 180ª Reunião Ordinária, sendo realizadas de forma conjunta no dia 26 de Agosto de 2021.

12. ANEXO I NORMAS COMPLEMENTARES

12.1 NC. TP. 01 – ACESSO FÍSICO E LÓGICO

12.1.1 OBJETIVO

Estabelecer controle de acesso físico e lógico no ambiente computacional da Taboãoprev.

12.1.2 DIRETRIZES GERAIS

a) Acesso Físico

I. Os controles de acesso físico visam restringir o acesso aos equipamentos, documentos e a proteção dos recursos computacionais, permitido apenas servidores da autarquia;

II. Todo o pessoal envolvido em trabalho de apoio tais como manutenção das instalações físicas, deve ser acompanhado de um servidor responsável;

III. O ingresso de visitantes deve ser controlado de tal forma a impedir o acesso destes às áreas de armazenamento e processamento de informações sensíveis, salvo acompanhados e com autorização de responsável.

b) Acesso Lógico

I. Os controles de acesso lógico são um conjunto de procedimentos, recursos e meios utilizados com a finalidade de prevenir e/ou obstruir ações de qualquer natureza que possam comprometer recursos computacionais, redes corporativas, aplicações e sistemas de informação;

II. Os sistemas da Taboãoprev devem possuir controle de acesso de modo a assegurar o uso apenas a servidores ou processos autorizados. A responsabilidade pela autorização ficará a cargo da Superintendência Autárquica que definirá quais sistemas os servidores terão acesso, de acordo com a necessidade ou atribuições a eles conferidas;

III. O servidor ao tomar posse ou ser nomeado para cargo na Taboãoprev deverá assinar uma "Declaração de Ciência e Compromisso a Política de Segurança da Informação – PSI", onde se comprometa em sua observância e acatamento.

IV. O acesso remoto aos recursos computacionais deve ser realizado adotando os mecanismos de segurança definidos para evitar ameaças à integridade e sigilo do serviço.

12.2 NC. TP. 02 – TRATAMENTO DA INFORMAÇÃO

12.2.1 OBJETIVO

Definir os requisitos e regras para classificação e tratamento da informação no ambiente de tecnologia da Taboãoprev.

12.2.2 DIRETRIZES GERAIS

a) A informação utilizada pela Taboãoprev é um bem que tem valor. Ela deve ser protegida, cuidada e gerenciada adequadamente com o objetivo de garantir a sua disponibilidade, integridade, confidencialidade, autenticidade e audibilidade, independente do meio de armazenamento ,processamento ou transmissão que esteja sendo utilizado;

b) Cada usuário deve acessar apenas as informações e os ambientes previamente autorizados. Qualquer tentativa de acesso a ambientes não autorizados será considerada uma violação desta Norma;

c) O acesso da informação armazenada e processada no ambiente de tecnologia é individual e intransferível. Esse acesso acontece através da identificação e autenticação do usuário;

d) Todos os procedimentos que a proteção da informação e continuidade de seu uso devem ser documentados, de tal forma que possibilite que a organização continue a operacionalização desses procedimentos;

e) Devem ser estabelecidos critérios para deleção segura de informações armazenadas em estações de trabalho e/ou outros dispositivos de armazenamento, como formatação de máquinas ou desmagnetização de discos, quando o equipamento for transferido para outro usuário ou descartado pela Taboãoprev para algum outro destino;

f) Toda informação crítica para o funcionamento da Taboãoprev deve possuir, pelo menos, uma cópia de segurança atualizada e guardada em local remoto, com proteção adequada.

12.3 NC. TP. 03 – CONTAS DE ACESSO E SENHAS

12.3.1 OBJETIVO

Estabelecer critérios para a disponibilização e administração do acesso aos serviços de tecnologia e informação da Taboãoprev, assim como estabelecer critérios relativos às senhas das respectivas contas.

12.3.2 DIRETRIZES GERAIS

a) Criação de Contas de Acesso

I. Todo cadastramento de conta de acesso à rede da Taboãoprev deve ser efetuado na posse ou nomeação do servidor da Taboãoprev, conforme a necessidade e de acordo com determinação da Superintendência Autárquica;

II. Todos os usuários devem assinar uma "Declaração de Ciência e Compromisso a Política de Segurança da Informação – PSI", onde se comprometa em sua observância e acatamento.

III. Qualquer anormalidade percebida pelo usuário quanto ao privilégio de seu acesso aos recursos de tecnologia da informação deve ser imediatamente comunicada à Diretoria Executiva.

b) Exclusão e Bloqueio de Contas de Acesso

I. A exclusão da conta de acesso do usuário deve ocorrer caso haja:
i. Falecimento do servidor;
ii. Aposentadoria do servidor; e
iii. Outros afastamentos que caracterizem encerramento do vínculo do servidor com a Taboãoprev;

II. As contas com privilégio de administração de rede devem ser utilizadas somente para execução das atividades correspondentes à administração do ambiente conforme as responsabilidades atribuídas, em equipamentos previamente definidos. As variáveis necessárias para acesso e administração devem ser de conhecimento restrito aos administradores dos equipamentos de rede e chefia respectiva.

c) Senhas

I. Todas as senhas, de usuários comuns, para autenticação na rede da Taboãoprev devem seguir os seguintes critérios mínimos:
i. Toda senha deve ser constituída de, no mínimo 8 caracteres sendo obrigatório o uso de caracteres alfanuméricos (letra e números);
ii. a senha não poderá conter parte do nome do usuário, por exemplo: se o usuário chama-se Jose da Silva, sua senha não pode conter partes do nome como "12221jose" ou "1212silv".

12.4 NC. TP. 04 – CORREIO ELETRÔNICO

12.4.1 OBJETIVO

A disponibilidade do serviço de correio eletrônico corporativo da Taboãoprev aos seus servidores.

12.4.2 DIRETRIZES GERAIS

a) O serviço de correio tem como finalidade o envio e o recebimento eletrônico de mensagens e documentos relacionados com as funções institucionais da Taboãoprev;

b) São usuários do serviço de correio eletrônico corporativo os servidores da Taboãoprev;

c) A concessão de contas de correio eletrônico será efetuada na posse ou nomeação do servidor;

d) É vedado o acesso pelo conteúdo das mensagens transmitidas por meio do serviço de correio eletrônico corporativo, salvo nas hipóteses previstas em lei;

e) O acesso indevido às informações tramitadas por meio do serviço de correio eletrônico corporativo, da Taboãoprev, ou contidas em seus ambientes, será punido na forma da lei;

f) O acesso ao serviço de correio eletrônico dar-se-á por meio de senha de uso pessoal e intransferível, vedada sua divulgação;

g) É vedado ao usuário o uso do serviço de correio eletrônico corporativo com o objetivo de:

I. Praticar crimes e infrações de qualquer natureza;
II. Executar ações nocivas contra outros recursos computacionais da Taboãoprev ou de redes externas;
III. Distribuir material obsceno, pornográfico, ofensivo, preconceituoso, discriminatório, ou de qualquer forma contrário à lei e aos bons costumes;
IV. Disseminar anúncios publicitários, mensagens de entretenimento e mensagens do tipo "corrente", vírus ou qualquer outro tipo de programa de computador que não seja destinado ao desempenho de suas funções ou que possam ser considerados nocivos ao ambiente de rede da Taboãoprev;
V. Emitir comunicados gerais com o caráter eminentemente associativo, sindical ou político-partidário;
VI. Enviar arquivos de áudio, vídeo ou animações, salvo os que tenham relação com as funções institucionais desempenhadas pela Taboãoprev;
VII. Executar outras atividades lesivas, tendentes a comprometer a intimidade de usuários, a segurança e a disponibilidade do sistema, ou a imagem institucional.

12.5 NC. TP. 05 – RECURSOS COMPUTACIONAIS

12.5.1 OBJETIVO

Estabelecer critérios e procedimentos para o uso dos recursos computacionais disponíveis aos usuários da Taboãoprev, assim como o controle, administração e requisitos mínimos desses recursos.

12.5.2 DIRETRIZES GERAIS

a) Recursos Computacionais em Geral

I. Os usuários devem ter acesso unicamente àqueles recursos computacionais que forem indispensáveis à realização de suas atividades na Taboãoprev;
II. A utilização dos recursos de tecnologia, com finalidade pessoal, é permitida, desde que seja em nível mínimo e que não viole a Política, as Normas Complementares e o Código de Ética da Instituição;
III. Os usuários são responsáveis pelos recursos computacionais por eles utilizados, devendo preservar a sua integridade e continuidade;
IV. Os ambientes onde se encontram instalados ou guardados os recursos computacionais devem permanecer protegidos mesmo na ausência dos usuários;
V. É vedado aos usuários da Taboãoprev utilizar a identificação e/ou senha de outro usuário para acessar ou utilizar um recurso computacional;
VI. É vedado aos usuários fazer uso de exploração de falhas de configuração, falhas de segurança ou tentar obter conhecimento de senhas especiais para alterar um Recurso Computacional;
VII. Tendo em vista a preservação do ambiente computacional da Taboãoprev, é vedado aos usuários o fornecimento de informações a terceiros sobre caraterísticas, funcionalidades e configurações dos recursos de tecnologia da informação disponíveis.

b) Estações de Trabalho

I. Estações de trabalho somente devem ser utilizadas para execução de atividades de interesse da Taboãoprev;
II. O usuário deve zelar pela conservação dos equipamentos de informática sob sua responsabilidade, não podendo fumar nem alimentar-se próximo a eles;
III. É vedado aos usuários abrir as estações de trabalho ou modificar a configuração do hardware;
IV. O usuário, sempre que se ausentar da estação de trabalho deve bloqueá-la para impedir o acesso não autorizado;
V. O usuário deve informar imediatamente a Diretoria Executiva quando identificada violação da integridade do equipamento por ele utilizado;
VI. A configuração do ambiente operacional da estação de trabalho somente poderá ser alterada por técnico autorizado pela Diretoria Executiva;
VII. O usuário deve ligar/desligar de forma adequada e segura o equipamento;
VIII. Caso o usuário identifique a necessidade de alguma atualização deverá comunicar à Diretoria Executiva;
IX. Todas as estações de trabalho deverão possuir o programa de antivírus homologado pela Taboãoprev;

X. O antivírus deve estar atualizado e com a autoproteção ativa na estação de trabalho;
XI. O usuário deve obrigatoriamente executar o antivírus nos dispositivos removíveis antes de sua abertura quando inseridos na estação de trabalho;
XII. O usuário deve cancelar o processo de verificação de vírus quando este for iniciado automaticamente na sua estação de trabalho;
XIII. Não é permitida a conexão de estações de trabalho particulares, portáteis ou não, à rede da Taboãoprev, exceto em casos de comprovada necessidade, situações nas quais deverá ser assegurada a devida adoção de padrões de segurança compatíveis com o disposto nessa norma.

c) Equipamentos Portáteis

I. Os equipamentos portáteis devem respeitar as mesmas regras estabelecidas para estações de trabalho;
II. Equipamentos portáteis de propriedade da Taboãoprev devem ser guardados em local seguro, com controle de acesso e garantia quanto à sua integridade;
III. Somente técnicos autorizados pela Taboãoprev devem configurar os equipamentos portáteis;
IV. O usuário deve evitar armazenar informações confidenciais em equipamentos portáteis da Taboãoprev.

d) Manutenção e Configuração

I. Toda solicitação de atendimento para instalação, suporte e configuração dos recursos computacionais deve ser efetuada mediante solicitação a Diretoria Executiva;
II. A equipe de atendimento deve estar devidamente identificada para a execução dos serviços de suporte técnico;
III. Nas dependências físicas da Taboãoprev somente é permitida a execução dos serviços de suporte técnico nos equipamentos de propriedade da instituição, sendo proibida a assistência técnica em equipamentos particulares;
IV. O usuário deve acompanhar o técnico durante a manutenção da sua estação de trabalho;
V. O usuário deve estar ciente da saída do equipamento de seu local de trabalho caso seja necessária a retirada do mesmo para manutenção;
VI. Todo recurso computacional que sair das dependências físicas da Taboãoprev por motivo de manutenção deverá ser registrado pelo responsável da unidade e deverá ter suas informações institucionais críticas previamente excluídas;
VII. O usuário deve manter o número, do registro do chamado ou número do documento de solicitação formal, do pedido de suporte por ele realizado para controle e acompanhamento do respectivo chamado.

12.6 NC. TP. 06 - UTILIZAÇÃO DA INTERNET

12.6.1 OBJETIVO

Estabelecer critérios para administração e utilização de acesso aos serviços de internet no âmbito da Taboãoprev.

12.6.2 DIRETRIZES GERAIS

a) Internet

I. São usuários da internet da Taboãoprev os servidores e estagiários da Taboãoprev;
II. O acesso a internet deve restringir-se à esfera profissional com conteúdo relacionado às atividades desempenhadas pela Taboãoprev, observando-se sempre a conduta compatível com a moralidade administrativa;
III. Cada usuário é responsável pelas ações e acessos realizados por meio de sua Conta de Acesso;
IV. Os usuários devem estar capacitados a utilizar os serviços de modo a garantir a sua utilização adequada;
V. É vedado o uso de provedores de acesso externos ou de qualquer outra forma de conexão não autorizada no ambiente da Taboãoprev;
VI. É vedado acessar páginas de conteúdo considerado ofensivo, ilegal ou impróprio, tais como:
   a. Pornografia, pedofilia, preconceitos, vandalismo, entre outros;
   b. Acessar ou obter na internet arquivos que apresentem vulnerabilidade de segurança ou possam comprometer, de alguma forma, a segurança e a integridade da rede da Taboãoprev;
   c. Uso recreativo da Internet em horário de expediente;
   d. Uso de Proxy anônimo;
   e. Acesso a salas de bate-papo (chats), exceto aqueles definidos como ferramenta de trabalho homologado pela Taboãoprev;
   f. Acesso a rádio e TV em tempo real, exceto os canais corporativos como por exemplo, a TV Escola;
   g. Acesso a jogos;
   h. Acesso a outros conteúdos notadamente fora do contexto do trabalho desenvolvido;
   i. Divulgação de informações confidenciais da instituição por meio de correio eletrônico, grupos ou listas de discussão, sistemas de mensageria ou bate-papo, blogs, microblogs, ou ferramentas semelhantes;
   j. Envio a destino externo de qualquer software licenciado a Taboãoprev ou dados de sua propriedade ou de seus usuários, salvo expressa e fundada autorização do responsável pela sua guarda;
   k. Contorno ou tentativa de contorno às políticas de bloqueios automaticamente aplicadas pelas ferramentas sistêmicas da Taboãoprev;
   l. Utilização de softwares de compartilhamento de conteúdos na modalidade peer-to-peer (P2P);
   m. Tráfego de quaisquer outros dados em desacordo com a lei ou capazes de prejudicar o desempenho dos serviços de tecnologia da informação da Taboãoprev.
VII. A ocorrência de qualquer hipótese de má utilização da internet deverá ser comunicada, de imediato a Diretoria Executiva;
VIII. Comprovada a utilização irregular, o usuário envolvido terá o seu acesso à internet bloqueado, sendo comunicado o fato à chefia imediata, podendo incorrer em processo administrativo disciplinar e nas sanções legalmente previstas, assegurados o contraditório e a ampla defesa.

12.7 NC. TP. 07 – PROCEDIMENTOS DE CONTINGÊNCIA

12.7.1 OBJETIVO

Estabelecer critérios para procedimentos de contingências, para realizar cópias de segurança dos sistemas de informação e de banco de dados no âmbito da Taboãoprev.

12.7.2 DIRETRIZES GERAIS

a) Os servidores da Taboãoprev são responsáveis por efetuar cópias de segurança (Backups) em suas estações de trabalho, de todos os arquivos, documentos eletrônicos e banco de dados, que sejam considerados de fundamental importância para a continuidade dos trabalhos na Taboãoprev;

b) Os serviços de backup dos diretórios dos "servidores de arquivos" da Taboãoprev serão realizados diariamente;

c) Sempre que possível um computador e/ou notebook estarão à disposição para substituir outro equipamento que apresente problemas;

d) Todos os backups serão salvos em HD externo, exclusivo para esta finalidade ou no sistema de nuvens, protegidos por senha, sob a responsabilidade dos servidores de cada setor.