POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

2ª EDIÇÃO 2019

1. INTRODUÇÃO

A informação utilizada pelo **INSTITUTO MUNICIPAL DE PREVIDÊNCIA DOS SERVIDORES PÚBLICOS DE ITAÚNA - IMP** é um bem que tem valor. A informação deve ser protegida, cuidada e gerenciada adequadamente com o objetivo de garantir sua disponibilidade, integridade, confidencialidade, legalidade e auditabilidade, independentemente do meio de armazenamento, processamento ou transmissão que esteja sendo utilizado.

O desenvolvimento e a implantação da Política de Segurança da Informação - PSI é uma importante ferramenta para combater ameaças aos ativos do Instituto. Esta PSI é um conjunto de diretrizes e orientações de procedimentos que visam conscientizar e orientar os empregados, clientes, parceiros, colaboradores e fornecedores para o uso seguro dos ativos do Instituto.

A Gestão de Continuidade de Negócios, disposta em norma específica, tem por objetivo, em relação à segurança da informação, garantir níveis adequados de disponibilidade, integridade, confidencialidade e autenticidade das informações essenciais ao funcionamento dos processos críticos do **Instituto Municipal de Previdência dos Servidores Públicos de Itaúna - IMP.**

2. OBJETIVOS

A Política de Segurança da Informação – PSI tem como objetivos:

I). Registrar os princípios e as diretrizes de segurança adotados pelo **IMP**, a serem observados por todos os seus integrantes, colaboradores, fornecedores, prestadores de serviços, membros dos colegiados e aplicados a todos os sistemas de informação e processos corporativos.

II) Definir o tratamento que deve ser dado às informações armazenadas, processadas ou transmitidas no ambiente convencional ou no ambiente tecnológico.

III) Preservar as informações do **IMP** quanto a:

a. **Confidencialidade:** propriedade que garante que a informação seja acessada somente pelas pessoas ou processos que tenham autorização para tal;

b. **Integridade:** propriedade que garante a não violação das informações com intuito de protegê-las contra alteração, gravação ou exclusão indevida, acidental ou proposital;
c. **Disponibilidade:** propriedade que garante que as informações estejam acessíveis às pessoas e aos processos autorizados, no momento requerido;
d. **Autenticidade:** propriedade que assegura a correspondência entre o autor de determinada informação e a pessoa, processo ou sistema a quem se atribui a autoria;

As orientações aqui apresentadas são os princípios fundamentais e representam como o **IMP** exige que a informação seja utilizada.

3. APLICAÇÕES DA PSI

As diretrizes aqui estabelecidas deverão ser seguidas por todos os seus integrantes, colaboradores, fornecedores, prestadores de serviços, membros dos colegiados, e se aplicam à informação em qualquer meio ou suporte.

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

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

4.PRINCÍPIOS DA PSI

Toda informação produzida ou recebida pelos colaboradores como resultado da atividade profissional pertence ao IMP. As exceções devem ser explícitas e formalizadas.

Os equipamentos de informática e comunicação, sistemas e informações são utilizados pelos colaboradores para a realização das atividades profissionais. Excepcionalmente, o uso pessoal dos recursos é permitido desde que não prejudique o desempenho dos sistemas e serviços.

Deverá constar em todos os contratos do IMP Cláusula de Confidencialidade, como

j. Os usuários deverão proteger o acesso a seus computadores através de tela de bloqueio a ser liberada mediante senha, quando os mesmos não estiverem em uso.

k. Além das cópias de segurança "backup" normalmente realizadas no servidor, será feita cópia de segurança adicional mantida em dispositivo externo com as informações codificadas (encriptografadas) em ambiente seguro para armazenagem fora do IMP.

l. O acesso à internet é feito com tecnologia fornecida por operadora especializada.

m. As informações em formato físico devem ser acondicionadas em armários específicos ou destruídas em triturador de papel, quando se tratar de documentos confidenciais a serem inutilizados.

6. DIRETRIZES PARA INFORMAÇÕES CONFIDENCIAIS

Objetivo:

Estabelecer responsabilidades e requisitos básicos de utilização dos dados do IMP.

Abrangência:

Aplicada aos ativos de informação e comunicação do IMP.

Conceito:

São consideradas informações confidenciais, para os fins desta Política, quaisquer informações das partes consideradas não disponíveis ao público ou reservadas.

a. É expressamente proibida a divulgação de informações dos Participantes;

b. Informações confidenciais, quando impressas, deverão ser retiradas imediatamente das impressoras;

c. Informações confidenciais impressas, quando não estiverem sendo utilizadas, deverão ser armazenadas em local fechado e seguro;

d. Nenhuma das informações confidenciais podem ser repassadas para terceiros sem consentimento por escrito da Diretoria Executiva do IMP.

7. DIRETRIZES PARA UTILIZAÇÃO DA REDE

Objetivo:

Estabelecer responsabilidades e requisitos básicos de utilização da rede do IMP.

Abrangência:

Aplicada a todos os usuários que utilizam a rede do IMP.

Conceito:

O acesso à rede permite aos usuários trafegar informações de internet, correio eletrônico e sistemas disponibilizados pelo IMP. Uma rede é definida como um conjunto de computadores interligados com o objetivo de permitir a transmissão das informações. Quanto à acessibilidade, podem ser públicas ou privadas. As redes privadas possibilitam a transmissão restrita de informações dentro do domínio de uma instituição pública ou privada; esta rede privada denomina-se intranet. As redes públicas permitem ao usuário a interconexão entre redes privadas. Quanto aos meios de transmissão, a informação pode ser enviada por conexões sem fio (Ex.: rádio e infravermelho) ou por conexões que utilizem cabeamento (Ex.: fibra ótica, cabo coaxial e par trançado).

a. O usuário é responsável pela própria e devida autenticação nos sistemas de redes disponibilizados pelo IMP, não podendo fornecer e/ou compartilhar seu usuário, senha e/ou acesso à rede com outros usuários;
b. O usuário está comprometido a utilizar as redes públicas e ou privadas do IMP para uso exclusivo de atividades relacionadas ao setor no qual o usuário pertence, excetuando-se quando previamente autorizado pelo responsável;
c. É proibida a utilização de proxies não autorizados que permitam o tráfego de informações a redes privadas externas;
d. É proibido o acesso a redes que disponibilizem conteúdos obscenos, pornográficos, eróticos, racistas, nazistas e de qualquer outro conteúdo que viole a lei;
e. O usuário deve garantir que as senhas de acesso à rede não sejam enviadas a outras pessoas, pois a senha é de uso pessoal, intransferível e sigilosa.

8. DIRETRIZES PARA INSTALAÇÃO E REMOÇÃO DE SOFTWARES

Objetivo:

Estabelecer um conjunto de diretrizes e recomendações aos diferentes usuários sobre os procedimentos de instalação e/ou remoção de programas nos equipamentos do IMP.

Abrangência:

Aplicada a todos os usuários do IMP que necessitam instalar e/ou remover programas dos computadores.

Conceito:

Todo e qualquer programa (software) são ferramentas e/ou instrumentos que auxiliam civis, empresas, governos, instituições de pesquisa, instituições de ensino, entre outros a realizar suas respectivas atividades. Os softwares podem ser executados em desktops, estações de trabalho, servidores, mainframes, roteadores, celulares, e em qualquer outro dispositivo computacional. Quanto aos tipos de programas eles podem ser: software de sistema e software de aplicativo. Os softwares de sistema são responsáveis pela integração entre máquina, periféricos e software de aplicativo. Os softwares de aplicativo são responsáveis pela interação entre o usuário e suas atividades. Alguns exemplos de software são: sistemas operacionais, planilhas eletrônicas, editores de texto, editores de imagens, visualizadores de arquivos, mensageiros instantâneos, correio eletrônico, dentre outros. O acesso de um aplicativo pode ser realizado localmente (quando acessados fisicamente na máquina utilizada) e/ou remotamente (quando os aplicativos são providos por outros equipamentos diferentes da máquina utilizada fisicamente).

a. O usuário é proibido de instalar todo e qualquer programa não autorizado no computador e qualquer outro dispositivo computacional pertencente ao IMP, salvo as instalações de programas que contenham prévia autorização da Diretoria Executiva. Este item também é aplicado a programas com conteúdo de atualização conhecidos como patches;
b. O usuário é proibido de remover toda e qualquer versão de software obsoleto, mesmo em casos onde exista uma versão atualizada da aplicação utilizada;
c. Caso o usuário necessite instalar ou remover qualquer software, deverá entrar em contato com o gerente administrativo.

9. DIRETRIZES PARA UTILIZAÇÃO DOS SISTEMAS CORPORATIVOS

Objetivo:

Estabelecer responsabilidades e requisitos básicos de utilização dos Sistemas Corporativos no ambiente de Tecnologia da Informação e Comunicação do IMP.

Abrangência:

Aplicada a todos os usuários que utilizam os Sistemas Corporativos do IMP.

Conceito:

Os Sistemas Corporativos são os sistemas utilizados na gestão do IMP de forma integrada, trazendo maior transparência, rapidez e confiabilidade para as informações, abrangendo todos os seguimentos da administração e permitindo o gerenciamento isolado de cada parte e a interligação desta com o todo, produzindo relatórios analíticos, sintéticos e estatísticos, sendo acessados através de uma rede interna ou externa.

a. É expressamente proibida a divulgação e/ou o compartilhamento indevido das informações contidas nos Sistemas Corporativos.
b. Todos os Usuários dos ativos de informação de propriedade do IMP, ao utilizarem esse serviço, deverão fazê-lo no estrito interesse do Instituto, mantendo uma conduta profissional.
c. O acesso às informações contidas nos Sistemas Corporativos deve ser efetuado sempre através de identificação segura (chave e senha).
d. Para cada usuário serão atribuídas permissões específicas, por módulo ou operação.
e. O usuário é pessoalmente responsável por todas as atividades realizadas por intermédio de sua chave de acesso.

10. DIRETRIZES PARA UTILIZAÇÃO DA INTERNET

Objetivo:

Estabelecer responsabilidades e requisitos básicos de utilização da Internet no ambiente de Tecnologia da Informação e Comunicação do IMP.

Abrangência:

Aplicada a todos os usuários que utilizam os recursos disponibilizados pelo IMP para

acesso à Internet.

Conceito:

Sob o aspecto de proteção e integridade dos sistemas de informação, a Internet é classificada como conexão de alto risco. Os usuários devem estar cientes, portanto, das peculiaridades da navegação na Internet, antes de acessá-la e de utilizar os seus recursos.

a. É expressamente proibida a divulgação e/ou o compartilhamento indevido de informações sigilosas em listas de discussão ou bate-papo.
b. Os usuários poderão fazer download de arquivos da Internet que sejam necessários ao desempenho de suas atividades desde que observado os termos de licença de uso e registro desses programas.
c. O usuário deve utilizar a Internet de forma adequada e diligente.
d. O usuário deve utilizar a Internet observando a conformidade com a lei, a moral, os bons costumes aceitos e a ordem pública.
e. O usuário deve se abster de utilizar a Internet com objetivos ou meio para a prática de atos ilícitos, proibidos pela lei ou pela presente Política, lesivos aos direitos e interesses do órgão público ou de terceiros, ou que, de qualquer forma, possam danificar, inutilizar, sobrecarregar ou deteriorar os recursos tecnológicos (hardware e software), bem como os documentos e arquivos de qualquer tipo, de seu uso ou de uso de terceiros.
f. O usuário é pessoalmente responsável por todas as atividades realizadas por intermédio de sua chave de acesso.
g. Não é permitida a utilização de software de peer-to-peer (P2P), tais como Torrent, Kazaa, Emule e afins.
h. Não é permitido acesso a sites de Proxy.

11. DIRETRIZES PARA UTILIZAÇÃO DE CORREIO ELETRÔNICO (E- MAIL)

Objetivo:

Estabelecer responsabilidades e requisitos básicos de uso dos serviços de Correio Eletrônico, no ambiente de Tecnologia da Informação e Comunicação (TIC) do IMP.

Abrangência:

Aplicada aos ativos de informação e comunicação do IMP.

Conceito:

Prover a comunicação é, sem dúvida, a essência das redes. As pessoas sempre procuraram se corresponder da maneira mais rápida e fácil possível. O correio eletrônico (e-mail) é a aplicação que mais ilustra esta procura, pois reúne, entre outros, estes atributos. Entretanto, a facilidade de correio eletrônico fornecido pelo IMP deve ser usada no interesse do serviço, podendo ser, ocasionalmente, utilizada para mensagens pessoais curtas e pouco frequentes.

a. Todos os Usuários dos ativos de informação de propriedade do IMP, ao utilizarem esse serviço, deverão fazê-lo no estrito interesse do instituto, mantendo uma conduta profissional.

b. Todas as contas de correio eletrônico terão uma titularidade, determinando a responsabilidade sobre a sua utilização.

d. Contas com inatividade por um período igual ou superior a 60 (sessenta) dias serão bloqueadas, a fim de evitar o recebimento de novas mensagens.
e. O usuário é o responsável direto pelas mensagens enviadas por intermédio do seu endereço de correio eletrônico;
f. O usuário deve utilizar o Correio Eletrônico de forma adequada e diligente;

- É vedada a utilização do Correio Eletrônico, nas situações abaixo:
- acesso não autorizado à caixa postal de outro usuário;
- envio, armazenamento e manuseio de material que contrarie o disposto na legislação vigente, a moral e os bons costumes e a ordem pública;

- envio, armazenamento e manuseio de material que caracterize a divulgação, incentivo ou prática de atos ilícitos, proibidos pela lei ou pela presente Política, lesivos aos direitos e interesses do IMP ou de terceiros, ou que, de qualquer forma, possam danificar, inutilizar, sobrecarregar ou deteriorar os recursos tecnológicos (hardware e software), bem como os documentos e arquivos de qualquer tipo, do usuário ou de terceiros;
- envio, armazenamento e manuseio de material que caracterize: promoção, divulgação ou incentivo a ameaças, difamação ou assédio a outras pessoas; assuntos de caráter obsceno; prática de qualquer tipo de discriminação relativa a raça, sexo ou credo religioso; distribuição de qualquer material que caracterize violação de direito autoral garantido por lei; uso para atividades com fins comerciais e o uso extensivo para

assuntos pessoais ou privados;

- envio de mensagens do tipo "corrente" e "spam";
- envio intencional de mensagens que contenham vírus eletrônico ou qualquer forma de rotinas de programação de computador, prejudiciais ou danosas;
- utilização de listas e/ou caderno de endereços do IMP para a distribuição de mensagens que não sejam de estrito interesse funcional e sem a devida permissão do responsável pelas listas e/ou caderno de endereços em questão.

12. DIRETRIZES PARA UTILIZAÇÃO DE DISPOSITIVOS MÓVEIS (CONSUMERIZAÇÃO)

Objetivo:

Estabelecer responsabilidades e requisitos básicos de utilização de dispositivos móveis no ambiente de Tecnologia da Informação e Comunicação do IMP.

Abrangência:

Aplicada a todos os usuários que utilizam os recursos disponibilizados pelo IMP.

Conceito:

Dispositivos móveis são equipamentos portáteis dotados de capacidade computacional, e dispositivos removíveis de memória para armazenamento, entre os quais se incluem, não se limitando a estes: notebooks, netbooks, smartphones, tablets, pen drives, USB drives, HD externos e cartões de memória;

a. É expressamente proibida a divulgação e/ou o compartilhamento indevido de informações sigilosas através de dispositivos móveis.
b. O usuário deve utilizar os dispositivos móveis de forma adequada e diligente, de forma a prevenir ações que possam danificar, inutilizar, sobrecarregar ou deteriorar os recursos tecnológicos (hardware e software), bem como os documentos e arquivos de qualquer tipo, de seu uso ou de uso de terceiros;
c. O usuário é pessoalmente responsável por todas as atividades realizadas por intermédio de dispositivos móveis, tanto por sua guarda quanto pelos conteúdos nele instalados.

13. DIRETRIZES PARA UTILIZAÇÃO DE ACESSO REMOTO À REDE DO IMP

Objetivo:

Estabelecer responsabilidades e requisitos básicos de utilização da rede do IMP através de acesso remoto.

Abrangência:

Aplicada a todos os usuários que utilizam a rede do IMP e/ou terceiros que utilizam serviços de acesso remoto.

Conceito:

A interconexão entre redes privadas a distância permite ao usuário utilizar de redes e serviços de redes disponibilizados por terceiros. O acesso a redes remotas disponibilizados por redes privadas externas permitem ao usuário acessar, utilizar e executar aplicações e sistemas operacionais disponibilizados naquele ambiente, desde que tenham acesso autorizado para isto. Por se tratar de um acesso entre redes privadas, a segurança e integridade da informação trafegada dependem das configurações da rede. Logo, este tópico tem como objetivo estipular um conjunto de diretrizes e recomendações aos diferentes usuários do IMP. A boa utilização destes serviços é de responsabilidade de cada usuário com seus respectivos privilégios. Cabe ressaltar que os serviços estão disponibilizados para o uso estritamente profissional e de interesse do IMP.

a. O usuário somente pode realizar acesso interativo entre redes onde a permissão esteja autorizada. A autorização depende das atividades profissionais relacionadas a função exercida;
b. O usuário deve utilizar somente o local e o ambiente físico aprovado pelo IMP;
c. O usuário externo deve configurar de forma adequada o firewall e a proteção antivírus na rede externa à rede do IMP;
d. O usuário somente poderá realizar as atividades em período estipulado pelo IMP.

14. DIRETRIZES PARA UTILIZAÇÃO DE ACESSO REMOTO AO HOSTING

Objetivo:

Estabelecer responsabilidades e requisitos básicos de utilização do Hosting Externo do IMP através de acesso remoto.

Abrangência:

Aplicada a todos os usuários que utilizam a rede do IMP e/ou terceiros que utilizam serviços de acesso remoto.

Conceito:

Para garantia da integridade dos dados do IMP e utilização em caso de contingência, as informações armazenadas na rede interna estão replicadas em servidores virtuais externos (nuvem). O acesso a redes remotas permite ao usuário acessar, utilizar e executar aplicações e sistemas operacionais disponibilizados naquele ambiente, desde que tenham acesso autorizado para isto. Este tópico tem como objetivo estipular um conjunto de diretrizes e recomendações aos diferentes usuários do IMP. A boa utilização destes serviços é de responsabilidade de cada usuário com seus respectivos privilégios. Cabe ressaltar que os serviços estão disponibilizados para o uso estritamente profissional e de interesse do IMP.

a. Por se tratar de solução de contingência devem utilizados de acordo com o estabelecido nos normativos específicos ;
b. O usuário somente poderá realizar as atividades em período estipulado pelo IMP.

15. DIRETRIZES PARA UTILIZAÇÃO DE CONTAS E SENHAS DE ACESSO

Objetivo:

Estabelecer requisitos básicos de utilização dos recursos computacionais que requerem autenticação por senhas.

Abrangência:

Aplicada a todos os usuários do IMP que utilizem recursos computacionais que requerem autenticação por senhas.

a. O usuário não deve armazenar as senhas anotadas em papel ou em arquivos, seja no computador ou em dispositivos móveis, de forma desprotegida ou

seja, sem utilizar um meio de proteção, como, por exemplo, criptografia;

b. As senhas de acesso tem caráter pessoal, e é intransferível, cabendo ao seu titular total responsabilidade quanto ao seu sigilo;
c. O usuário está proibido de utilizar contas e senhas de acesso pertencentes a outros usuários;
d. O usuário deverá realizar a troca de suas senhas de acesso, pelo menos, semestralmente.

16. CONDIÇÕES GERAIS

Somente poderão acessar os Sistemas Corporativos e/ou a Internet usuários que tenham sido credenciados com suas senhas de acesso.

Cada Gerência do instituto deverá, através de e-mail, solicitar à Equipe da Gerência Superior de Tecnologia da Informação da Prefeitura Municipal de Itaúna a liberação de acesso a novos usuários, definindo os serviços que deverão ser credenciados, justificando quanto a necessidade do referido usuário utilizar- se deste recurso.

A senha de acesso tem caráter pessoal, e é intransferível, cabendo ao seu titular total responsabilidade quanto seu sigilo.

A prática de compartilhamento de senhas de acesso é terminantemente proibida e o titular que fornecer sua senha a outrem responderá pelas infrações por este cometidas, estando passível das penalidades aqui previstas.

Conceito:

Todo usuário do IMP possui para cada recurso computacional (estações de trabalho, sistemas, etc.) um identificador único provido pela Instituto, sendo que para cada identificador é associada uma senha que permite o acesso ao recurso com seus devidos privilégios.

a. Caso o usuário desconfie que sua senha não é mais segura, ou de seu domínio exclusivo, poderá solicitar à Equipe da Gerência Superior de Tecnologia da Informação a alteração desta.
b. Os usuários deverão tomar conhecimento formal desta Política, além de ser concedido treinamento para facilitar o entendimento e a comunicação.
c. Todos os usuários (empregados e fornecedores) mesmo que em caráter temporário, deverão assinar termo de ciência e concordância desta Política,

declarando ter conhecimento de suas responsabilidades no manuseio de hardware, software e acesso à internet.

d. A Equipe da Gerência Superior de Tecnologia da Informação deverá, pelo menos semestralmente, efetuar testes de verificação de acesso ao sistema e bloqueio automático de senha.
e. Deverão ser observados os princípios constantes do Código de Ética e Conduta do Instituto.
f. Por ocasião do desligamento de qualquer servidor, a Equipe da Gerência Superior de Tecnologia da Informação deverá ser comunicada para providenciar o imediato cancelamento de todas as senhas de acesso aos sistemas corporativos bem como do correio eletrônico.

17. PENALIDADES

O usuário que infringir qualquer uma das diretrizes de segurança expostas neste instrumento estará passível das seguintes penalidades:

a. Advertência verbal;
b. Descredenciamento da senha de acesso à Internet;
c. Cancelamento da caixa de e-mail;
d. Desativação do ponto de rede do usuário;
e. O(s) usuário(s) infrator (es) deverá (ão) ser notificado(s) e a ocorrência da transgressão imediatamente comunicada, pela Equipe da Gerência Superior de Tecnologia da Informação da PMI , à Gerência correspondente e à Diretoria Geral, para aplicação das penalidades previstas no Código de Ética do IMP.

18. MEMBROS DA EQUIPE DA GERÊNCIA SUPERIOR DE TECNOLOGIA DA INFORMAÇÃO

A Equipe da Gerência Superior de Tecnologia da Informação da Prefeitura Municipal de Itaúna, será diretamente responsável pela implantação e implementação da presente política, devendo reportar-se à referida Equipe todo e qualquer usuário e/ou área para tratar de assuntos pertinentes à segurança da informação de que trata este instrumento.

19. PLANO DE CONTINGENCIA

Em consonância com a Política de Segurança da Informação, a Diretoria Geral do IMP estabelece com este Ato, uma política de cópias de segurança (backup) e restauração de arquivos digitais armazenados no seu parque tecnológico promovendo o seu Plano de Contingencia.

19.1. Objetivo:

Preservar a integridade e a disponibilidade de todas as informações sensíveis do Instituto Municipal de Previdência dos Servidores Públicos de Itaúna, garantindo sua restauração e operacionalidade no menor tempo possível, principalmente havendo indisponibilidade de serviços que dependam da operação de recuperação.

19.2. Orientações Gerais:

Cabe a Equipe da Gerência Superior de Tecnologia da Informação da Prefeitura Municipal de Itaúna prever a realização de testes periódicos de restauração, no intuito de averiguar os processos de backup e estabelecer melhorias.

A administração dos backups também deve ser orientada para que seus trabalhos respeitem as janelas para execução, inclusive realizando previsão para a ampliação da capacidade dos dispositivos envolvidos no armazenamento.

As mídias (ou dispositivos de armazenamento) deverão ser armazenadas em cofre das estruturas da Sala de Servidores do IMP e do Data Center da Prefeitura Municipal de Itaúna.

As mídias defeituosas ou inservíveis serão encaminhadas para picotagem, incineração, procedimentos de sobrescrita de dados remanescentes (disco rígido) ou outro procedimento que impossibilite a recuperação dos dados por terceiros.

As solicitações de restauração de arquivos deverão ser abertas formalmente através de "Demanda" que deverá conter os nomes dos arquivos e pastas que deverão ser recuperados e, principalmente, a data do arquivo que se pretende ter acesso.

19.3. Cumprimento, sanções e penalidades:

Todos os servidores, membros de órgãos colegiados do IMP, fornecedores e prestadores de serviços declaram conhecer este documento e em decorrência devem ficam cientes de sua responsabilidade pessoal no cumprimento das regras conforme prescrito neste termo.

Em caso de descumprimento, o IMP poderá realizar ações disciplinares, rompimentos contratuais ou outras medidas consideradas apropriadas, de acordo com a gravidade do ato.

Periodicamente, serão efetuadas avaliações sobre o nível de aderência às normas e aos procedimentos definidos e suas diretrizes.

19.4. Princípios

Constituem-se os princípios da Política de Backup de Dados do IMP :

a) Proteger todos os programas e dados lógicos registrados e/ou gerados em sua infraestrutura de TI, contra perda, modificação ou destruição permanente;

b) Assegurar que todos os programas e dados lógicos sejam devidamente salvaguardados segundo seus critérios de retenção e frequência de atualização;

c) Garantir a continuidade operacional dos serviços do IMP;

d) Cumprir as leis e normas que regulamentam as atividades do IMP e seu segmento de atuação.

19.5. Responsabilidades

a) Gerência Superior de Tecnologia da Informação

- Adotar e praticar as diretrizes desta Política;

- Monitorar e fazer a gestão dos dados e mídias manipuladas neste processo;

- Reavaliar e promover uma contínua evolução das diretrizes e procedimentos desta Política;

- Difundir as diretrizes e procedimentos na instituição.

b) Gerentes, servidores, e usuários de TI do Instituto Municipal de Previdência dos Servidores Públicos de Itaúna

- Adotar e praticar os procedimentos definidos nesta Política;

- Difundir e fazer valer as diretrizes e regras desta Política para todos usuários diretos e indiretos.

19.6. Diretrizes

19.6.1. Das mídias de armazenamento de Backup

Todas as mídias devem receber um nível adequado de proteção e serem protegidos a sua integridade e disponibilidade de acordo com a classificação dos dados nela contido.

Para estes ativos, deverão ser adotados controles para evitar o acesso ou qualquer atividade que não estejam devidamente autorizadas.

19.6.2. Da Organização e dos Controles Gerais

Deverá ser estabelecido um processo para gerenciar os acessos e as atividades com estes dados. Dentre os controles específicos, deverão ser estabelecidos, entre outros:

a) Todo acesso a dados de Backup deverá ser previamente registrado e justificado pelo aplicativo de "Demandas" no sistema de "Work Flow" da Gerência Superior de Tecnologia da Informação da Prefeitura Municipal de Itaúna. Deverão ser informados: forma de acesso, motivo do acesso, relação nome e identificação de todas as pessoas que farão o acesso, data e horário previsto de início e fim deste acesso;

b) Os registros de acesso deverão ser retidos.

19.6.3. Da Conformidade

O uso e a gestão do sistema de Controle de Backup do IMP deverão estar em conformidade com os requisitos legais ou de segurança da informação.

20. VIGÊNCIA, VALIDADE E ATUALIZAÇÕES

A presente política passa a vigorar a partir da data de sua publicação sendo válida por tempo indeterminado.

Após a implantação desta Política, para que ela continue sendo satisfatória para o Instituto serão implantados controles de melhoria continua, ou seja, deverão ser realizadas revisões periódicas ou sempre que acontecer uma falha de segurança de nível médio ou grave.

GLOSSÁRIO

BACK-UP - Cópia de dados de um dispositivo de armazenamento a outro.

FIREWALL - Dispositivo de uma rede de computadores que tem por objetivo aplicar uma política de segurança a um determinado ponto da rede.

LOG - Registro de eventos em um sistema de computadores.

PATCHES - Programas criados para atualizar ou corrigir um software.

PEER-TO-PEER (P2P) - Arquitetura de redes de computadores onde cada um dos pontos ou nós da rede funciona tanto como cliente quanto como servidor, permitindo compartilhamentos de serviços e dados sem a necessidade de um servidor central.

PROXIES - Servidor intermediário que atende a requisições repassando os dados do cliente à frente.

SERVIDOR - Sistema de computação centralizada que fornece serviços a uma rede de computadores.

SPAN - Mensagem de correio eletrônico publicada em massa com fins publicitários.

21- Controle de datas de emissão e Revisão:

Elaborado por	Aprovado por	Nº Revisão	Data
Jarbas Fraguas / Eduardo Lichirgu	**Cláudio Silva Machado**	**000**	**08/11/2019**

Histórico das alterações		
Data	**Revisão**	**Histórico**
08/11/2019	**000**	**Implantação da Política de Segurança da Informação/2019**
10/08/2020	**001**	**2ª Edição da Política de Segurança da Informação - 2020**

Heli de Souza Maia
Diretor Geral do IMP
Matrícula 089-7