Instituto de Previdência Municipal de Praia Grande

POLITICA DE SEGURANÇA DA INFORMAÇÃO

Autores:

Regina Mainente
Superintendente

Ricardo Pereira da Silva
Controlador Interno

Ano de 2015

Instituto de Previdência Municipal de Praia Grande

Índice

Instituto de Previdência Municipal de Praia Grande

1. APRESENTAÇÃO:

Um programa de conscientização sobre segurança da informação tem como objetivo principal influenciar servidores e colaboradores a mudarem seus hábitos, bem como criar a consciência de que todos são corresponsáveis pela Segurança da Informação. Esse processo de conscientização deve ser contínuo, para manter os usuários alertas e para prepará-los para os novos riscos e ameaças que surgem a cada dia. Além dos aspectos gerais de Segurança da Informação, cada área deve ter um treinamento adequado a sua realidade. As políticas podem ser gerais, aplicadas a todos, ou específicas, aplicadas nas situações em que é necessária a existência de políticas e treinamentos específicos para determinados cargos ou grupos distintos dentro da organização.

Desejamos que a leitura deste material seja proveitosa e que as orientações aqui repassadas façam parte do seu cotidiano.

2. INTRODUÇÃO:

De acordo com Campos, (2007, p. 21).

(...)

"A informação é elemento essencial para todos os processos de negocio da organização, sendo, portanto, um bem ou ativo de grande valor". Logo, pode-se dizer que a informação se tornou o ativo mais valioso das organizações, podendo ser alvo de uma série de ameaças com a finalidade de explorar as vulnerabilidades e causar prejuízos consideráveis. Portanto, faz-se necessária a implementação de políticas de se segurança da informação que busquem reduzir as chances de fraudes ou perda de informações.

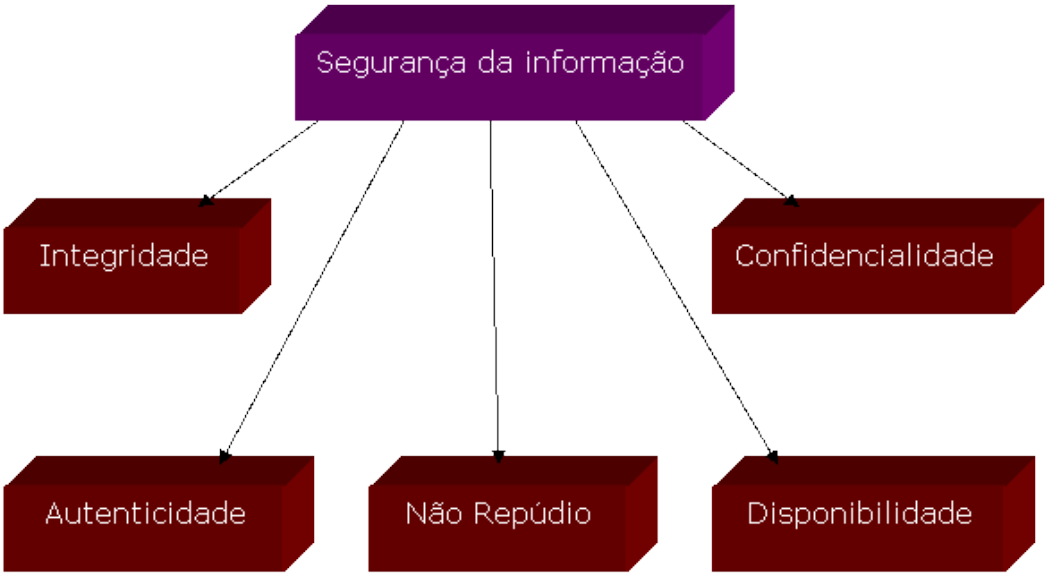
3. PARA QUE SERVE A SEGURANÇA DA INFORMAÇÃO?

A Segurança da Informação é necessária para garantir a proteção das informações corporativas ou pessoais, assegurando que nenhuma informação seja alterada ou utilizada indevidamente.

A Segurança da Informação é garantida por meio da preservação de dos cinco pilares básicos.

4. PILARES DA SEGURANÇA DA INFORMAÇÃO:

- **Confidencialidade:** É a garantia de que somente pessoas autorizadas terão acesso à informação;
- **Integridade**: É a garantia de que a informação mantém as características originais estabelecidas por seu proprietário, ou seja, de que não foi modificada ou alterada de forma indevida;
- **Disponibilidade**: É a garantia de que a informação estará pronta para o uso (por pessoas autorizadas) quando for necessária;
- **Autenticidade:** É a garantia de que a informação vem da fonte anunciada, ou seja, de que o autor da informação é realmente quem diz ser e,
- **Não repúdio:** É a garantia de que a pessoa não negue ter assinado ou criado a informação.



5. CONCEITO:

A Política de Segurança da Informação (PSI) pode ser definida como conjunto de normas, métodos e procedimentos utilizados para a manutenção da segurança da informação, devendo ser formalizada e divulgada a todos os usuários que fazem uso dos ativos de informação.

6. FINALIDADE:

A Política de Segurança da Informação tem por finalidade estabelecer as diretrizes para a segurança do manuseio, tratamento e controle e para a proteção dos dados, informações de conhecimentos produzidos, armazenados ou transmitidos, por qualquer meio pelos sistemas de informação.

7. OBJETIVO:

O objetivo da Política de Segurança da Informação é estabelecer diretrizes que permitam aos usuários do IPMPG seguirem padrões de comportamento relacionados à segurança adequados as necessidades de negócio da informação, bem como a implementação de controle e processos para seu atendimentos.

8. DA IMPORTANCIA:

"Atualmente, a PSI é adotada em grande parte das organizações em todo o mundo, inclusive no Brasil. Mesmo aquelas empresas que ainda não tem uma política efetiva, reconhecem a necessidade de elaborar e implementar uma". (CAMPOS, 2007, P. 131). A política de segurança da informação deve estabelecer como será efetuado o acesso as informações de todas as formas possíveis, seja ela internamente ou externamente, e quais os tipos de mídias poderão transportar e ter acesso a esta informação. A política deve especificar os mecanismos através dos quais estes requisitos podem ser alocados.

9. DA APLICAÇÃO AOS SERVIDORES:

Essa Política aplica-se a todos os servidores do IPMPG e demais agentes públicos ou particulares que, oficialmente, executem atividade vinculada à atuação institucional.

10. DOS CONCEITOS E DEFINIÇÕES BÁSICAS:

Para os fins dessa Política, considera-se:

- **Agente responsável:** Servidor Público ocupante de cargo efetivo ou em comissão;
- **Ameaça:** conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização;
- **Análise/avaliação de riscos:** processo completo de análise e avaliação de riscos;
- **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;
- **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;
- **Download:** (Baixar) copiar arquivos de um servidor (site) na internet para um computador pessoal;
- **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;
- **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.
- **Logon:** Procedimento de identificação e autenticação do usuário nos Recursos de Tecnologia da Informação. É pessoal e intransferível;
- **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;
- **Servidor de Rede:** recurso de TI com a finalidade de disponibilizar ou gerenciar serviços ou sistemas informáticos;
- **Servidor** - pessoa legalmente investida em cargo público;

- **Software:** são todos os programas existentes em um computador, como sistema operacional, aplicativos, entre outros;
- **SGSI:** É um sistema de gestão desenvolvido para a segurança da informação de uma organização, baseado em uma abordagem de riscos do negócio e,
- **Site:** Conjunto de páginas virtuais dinâmicas ou estáticas, que tem como principal objetivo fazer a divulgação da instituição.

11. DAS ORIENTAÇÕES:

Toda informação que é acessada, transmitida, recebida ou produzida com recursos tecnológicos oferecidos pelo Instituto, está sujeita a monitoramento que podem envolver inspeção física de equipamentos e registro de acessos à internet. Como os equipamentos, tecnologias e serviços fornecidos para o acesso à internet e ao e-mail são propriedade da instituição, ela tem o direito de monitorar, inspecionar e bloquear qualquer arquivo, site, correio eletrônico, domínio ou aplicação armazenados na rede/internet, que estejam em disco local na estação ou em áreas privadas da rede.

O uso indevido de qualquer recurso para atividades ilícitas ou que cause danos a terceiros será considerado violação às regras internas e terá as consequências previstas na legislação civil e criminal. Nesses casos, a instituição cooperará ativamente com as autoridades competentes.

A internet disponibilizada aos servidores não deve ser utilizada para a exposição de conteúdo íntimo ou de vida privada, tampouco vexatório, lembrando que o ambiente está sujeito a monitoramento. Na hipótese do uso indevido dos recursos disponibilizados, o usuário ficará ciente de que o conteúdo poderá ser retirado dos equipamentos independentemente de aviso prévio.

12. DO USO DA INTERNET:

O acesso a rede mundial de computadores e seus serviços utilizando os recursos do IPMPG ficam sujeito as seguintes regras abaixo:

- O acesso à Internet é proibido a pessoas que não pertençam ao quadro de servidores do IPMPG, salvo os autorizados;

- Fica extremamente proibido os sites que contenham conteúdo de material pornográficos, pedofilia, material que faça apologia as atividades criminosas e demais conteúdos semelhantes que afronte os bons costumes;

- Caso necessário, haverá bloqueios de acesso que comprometam o bom desempenho da rede ou perturbe o andamento dos trabalhos, domínios que comprometam o uso de banda e ofereçam riscos à segurança da rede e,

13. DO CORREIO ELETRÔNICO:

Os servidores poderá utilizar o correio eletrônico desde que essa ferramenta não seja utilizada de modo indevido, ilegal ou antiético.

Os servidores NÃO poderão utilizar o serviço de correio eletrônico para:

- Modificar arquivos ou assumir, sem autorização, a identidade de outro usuário;
- Prejudicar intencionalmente usuários da internet, através do envio de programas e de acesso não autorizados a computadores, ou de alterações de arquivos de programas;
- Utilizar-se do serviço de propriedade deste Instituto, desvirtuando sua finalidade com o intuito de cometer fraude;
- Utilizar o serviço de correio eletrônico de qualquer forma a participar em atividades de pesquisa comercial correntes, lixo eletrônico ou quaisquer mensagens periódicas ou não solicitadas (SPAM);
- Difamar, ofender, perseguir ou ameaçar ou de qualquer outra forma violar os direitos de terceiros;
- Enviar arquivos que contenham vírus, cavalos de troias, worm, arquivos corrompidos ou quaisquer outros softwares ou programas semelhantes que possam danificar a operação de outros computadores ou a propriedade de terceiros;
- Veicular, incitar ou estimular a pedofilia e similares;

14. DO SERVIDOR E ACESSO À REDE

O servidor do IPMPG deve ser utilizado seguindo as seguintes normas:

- Os usuários devem receber acesso somente aos serviços que tenham sido especificamente autorizados a usar.
- É obrigatório armazenar os arquivos inerentes ao IPMPG no servidor de arquivos para garantir a copia de segurança dos mesmo;
- É proibido o uso do servidor de arquivos para armazenar informações de cunho pessoal;
- Os arquivos gravados em diretórios temporários e públicos do servidor e das estações de trabalho podem ser acessados por todos os usuários que utilizarem a rede, portanto não se pode garantir sua integridade e disponibilidade;

- Não é permitido criar e/ou remover arquivos fora da área alocada ao usuário e/ou que venham a comprometer o desempenho e funcionamento da estrutura tecnológica;

- O usuário deve fazer manutenções periódicas no diretório pessoal, evitando acumulo de arquivos desnecessários;

- São de responsabilidade do usuário as informações em seu diretório pessoal, sendo que o mesmo deve evitar o acumulo de arquivos desnecessários e,

- As contas podem ser monitoradas pela Diretoria responsável, com o objetivo de verificar possíveis irregularidades no armazenamento ou manutenção dos arquivos nos diretórios pessoais.

15. DAS REGRAS GERAIS:

- Não são permitidas alterações das configurações da rede de inicialização das maquinas bem como as modificações que possam trazer algum problema futuro;

- A utilização de equipamentos de informática particulares na rede, só será liberada mediante autorização e vistoria no equipamento para saber se o mesmo atende aos requisitos mínimos de segurança exigidos, sendo ao final emitido o termo de autorização de uso de equipamentos particulares;

- Quando o servidor for transferido entre departamentos, o responsável pelo departamento deve certifica-se de que todos os direitos de acesso aos sistemas e outros controles de segurança serão necessários na sua nova função, e informar ao departamento de recursos humanos qualquer modificação necessária através de formulário especifico;

- Quando ocorrer a nomeação/contratação/exoneração/ demissão do servidor, a diretoria administrativa deverá providenciar a ativação ou desativação dos acessos do usuário a qualquer recurso da rede corporativa;

- É proibida a instalação ou remoção de softwares que não forem devidamente acompanhados pelo Diretor Administrativo e/ou responsável pelo setor de informática;

- O uso e manuseio, alteração, reposição de equipamento defeituoso será executado unicamente pelo responsável pelo setor da informática;

- É de exclusividade do responsável pelo setor da informática a troca de suprimentos de impressão como cartuchos, toners ou qualquer outro suprimento relativos a impressoras;

- É proibida a manutenção de equipamentos de informática particulares dentro das dependências do IPMPG e,

- Todo arquivo em mídia proveniente de entidade externa ao IPMPG deve ser verificado por programas antivírus. Todo arquivo recebido/obtido através do ambiente internet deve ser verificado por programa antivírus. O usuário não pode em hipótese alguma, desabilitar o programa antivírus instalado nas estações de trabalho.

16. DOS USUÁRIOS:

- Todo servidor do IPMPG terá direito a uma senha de acesso a rede corporativa e uma conta de email do Instituto;

- O acesso a quaisquer outros serviços ou sistemas providos pelo IPMPG ou por outros órgãos da administração direta devera ser solicitado a Superintendente pelo Diretor do departamento onde o usuário esta lotado;

- O usuário é o único responsável pelo uso da sua identificação (login e senha), quaisquer ações praticadas durante a utilização desta identificação será de sua inteira responsabilidade;

- O usuário não deverá compartilhar sua senha com outros usuários. Caso, o usuário perceba que outro usuário possa estar utilizando seu login de acesso, o mesmo deverá informar imediatamente o responsável pelo setor da informática, para efetuar a troca da senha e auditoria das atividades executadas com este login e,

- Antes de ausentar-se do local de trabalho,o usuário deverá fechar todos os programas em uso, efetuar o logoff da rede ou fazer o bloqueio do computador através do comando Ctrl + Alt + Del, evitando o uso dos recursos de TI por pessoas não autorizadas.

17. DAS RESPONSABILIDADES:

A responsabilidade referente a segurança da informação é atribuição do Diretor Administrativo, juntamente com o servidor responsável pelo setor de Informática da Autarquia, devendo comunicar a Superintendência e ao Controlador Interno ao constatar qualquer irregularidade.

18. DAS PENALIDADES:

O não cumprimento pelos servidores neste documento, seja isolada ou cumulativamente, poderá ensejar, de acordo com a infração cometida, as seguintes punições:

- Comunicação de Descumprimento - Será encaminhado ao funcionário, por e-mail, notificação informando o descumprimento da norma, com a indicação precisa da violação praticada e, em caso de reincidência, será enviada também, uma cópia para a respectiva chefia.

- Advertência ou Suspensão - A pena de advertência ou suspensão será aplicada nos casos legais e após regular apreciação através de processo administrativo disciplinar.

Em, 09 de Junho de 2015.

Regina Mainente
Superintendente

Ricardo Pereira da Silva
Controlador Interno

Douglas Gianotti
Diretor Administrativo

David Góes Aiub
Responsável pelo Setor de Informática