Manual de Políticas de Segurança da Informação

Instituto de Previdência dos
Servidores Municipais de Cabedelo
IPSEMC

Manual de Políticas de Segurança da Informação
2013

IPSEMC

ORIZANDO O SEU FUTURO

unicipais de Cabedelo

Presidente do IPSEMC
Léa Santana Praxedes

Diagramação
Jackson Angelo Pereira

Programador Visual
Jackson Angelo Pereira

Projeto Gráfico
Ana Lúcia Carvalho de Souza
Arturo Rodrigues Felinto
Jackson Angelo Pereira
Léa Santana Praxedes

Revisão de Linguagem
Leni Santana Praxedes

Consultores
Ana Lúcia Carvalho de Souza
Arturo Rodrigues Felinto

Produção Gráfica
Waldemar Pinho Neto

Editora
Grafique

Cabedelo, 02 de outubro de 2013.

MESA DIRETORA PREVIDENCIÁRIA DO IPSEMC

José Maria de Lucena Filho
Prefeito

Léa Santana Praxedes
Presidente

Ana Lúcia Carvalho de Souza
Assessora de Des. Institucional e Controle Interno – Consultora

Arturo Rodrigues Felinto
Consultor

Carlos Eduardo Toscano Leite Ferreira
Assessor Jurídico

Cristiane J. Felinto Brandão da Silva
Coordenadora Administrativa

Erivaldo de Lima Silva
Coordenador de Diligências

Fátima Maria de Araújo Pereira
Diretora de Benefícios

Ítalo Beltrão de Lucena Córdula
Assessor de Informática

João Thomaz da Silva Neto
Diretor Administrativo-Financeiro

Jackson Angelo Pereira
Chefe do Setor de Proc. de Dados

Maria Regina da Silva Dutra
Coordenadora de Recursos Humanos

CONSELHO PREVIDENCIÁRIO DO IPSEMC

Léa Santana Praxedes
Presidente

Ângela Maria Moreira Neves
Conselheira
Representante do Poder Executivo

Auzélia Marinho de Farias
Conselheira
Representante dos Servidores Inativos do Município

Euzo da Cunha Chaves
Conselheiro
Representante dos Servidores Ativos do Município

Maria das Graças Carlos Resende
Conselheira
Representante do Poder Legislativo Municipal

Wilma Alves de Lima
Conselheira
Representante dos Servidores Ativos
da Câmara Municipal

Controle do Documento

Nome	**Manual de Políticas de Segurança da Informação**	**Versão**	**1.0**
Publicado em	02.10.2013	Revisão em	
Aprovado por	Comissão de Políticas de Segurança da Informação do IPSEMC	Data	02.10.2013
Circulação	Circulação interna para todos os servidores do IPSEMC e externa aos usuários das informações a parceiros e a visitantes		

IPSEMC

ORIZANDO O SEU FUTURO

unicipais de Cabedelo

Sobre o IPSEMC

A Constituição de 1988 impôs à União a adoção de um Regime Jurídico Único, havendo na época, o entendimento legal de que o único regime que caberia aos servidores seria o estatutário.

A Constituição também impôs o pagamento de aposentadoria integral aos seus servidores, possibilitando que os entes federativos criassem seus regimes próprios de previdência. Em 1993 o cenário nacional apresentava-se muito caótico, principalmente pela ausência de uma legislação que disciplinasse a questão, além do insucesso das experiências obtidas pelos Estados e Municípios, os quais abrigaram sob o mesmo manto a previdência e a assistência à saúde dos servidores e familiares, sem a devida previsão orçamentária. Alguns regimes previdenciários só previam contribuição para pagamentos de pensões e assistência à saúde, cabendo aos cofres públicos o pagamento das aposentadorias, o que acabou por inviabilizar muitas administrações públicas. O Prefeito José Francisco Régis, à época, com ampla visão administrativa, compreendeu a necessidade de se criar um sistema de previdência para os servidores municipais, objetivando assegurar o direito constitucional a uma aposentadoria integral de forma a não comprometer as finanças públicas do Município de Cabedelo.

Assim, foi constituído um grupo de trabalho que durante dois anos estudou, pesquisou, realizou cursos, elaborou um anteprojeto de lei, promoveu discussões internas bem aprofundadas, o que ocasionou por várias vezes a re-elaboração do anteprojeto de lei, pois o processo de discussão assim o exigia. Destacam-se a participação da Secretaria de Administração e da Procuradoria Geral do Município que, de forma muito responsável, contribuiu significativamente para esse processo.

Como resultado deste desafiador esforço, em 23 de julho de 1993, é criado o Instituto de Previdência dos Servidores Públicos do Município de Cabedelo (Ipsemc), pela LEI nº 687/93, a qual passou a vigorar em 28/07/93 - publicada no Diário Oficial do Estado - DOE. O tempo, o dia a dia, a Lei 9717/98 e a Emenda Constitucional nº 20/98 trouxeram a necessidade de adequação da legislação do Ipsemc, o que foi concretizado pela Lei nº 1000/2000 e, em 22/08/2008 foi atualizada e consolidada pela Lei 1.412/2008 e publicada no DOE.

Sumário

Resolução Normativa

RESOLUÇÃO Nº 004/13 DE 02 DE OUTUBRO DE 2013

ESTABELECE O MANUAL DE POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO DO IPSEMC E DELIBERA OUTRAS PROVIDÊNCIAS.

A PRESIDENTE DO INSTITUTO DE PREVIDÊNCIA DOS SERVIDORES MUNICIPAIS DE CABEDELO – IPSEMC, Município de Cabedelo, usando das atribuições que lhe são conferidas pelas Leis n°s 687/93 e 1.412/98, em consonância com o Planejamento Estratégico do IPSEMC - 2012/2017,

CONSIDERANDO o que ficou definido no Planejamento Estratégico do IPSEMC para o período 2012-2017;

CONSIDERANDO o que consta na Estratégia 4 – Programação da Tecnologia da Informação e Comunicação; O.E. 1 – Desenvolver o Projeto de Segurança da Informação do IPSEMC e da Meta 1 – Desenvolver o Projeto de Segurança da Informação do IPSEMC até junho/ 2013;

CONSIDERANDO o que consta da Portaria nº 20/2013, datada de 28 de maio de 2013;

CONSIDERANDO, ainda, a aprovação, por unanimidade, da equipe previdenciária em última reunião realizada no dia 19 de setembro de 2013, junto à Comissão de Políticas de Segurança da Informação;

R E S O L V E:

Art. 1º Aprovar o Manual de Políticas de Segurança da Informação do Instituto de Previdência dos Servidores Municipais de Cabedelo – IPSEMC.

Art. 2º O Manual de Políticas de Segurança da Informação do IPSEMC tem por finalidades:

a) Estabelecer as políticas de adoção de softwares livres e outras boas práticas de gestão da informação;
b) Definir as responsabilidades da Comissão de Políticas de Segurança da Informação - CPSI do IPSEMC, bem como dos seus colaboradores no que concerne à administração, proteção e uso dos recursos informacionais do Instituto;
c) Descrever as políticas de proteção das informações contra acesso não autorizado, manutenção da confidencialidade, integridade e disponibilidade da informação armazenada e assegurar que as medidas legislativas e regulamentares e outros requisitos sejam cumpridos; e
d) Otimizar o gerenciamento de riscos, prevenir e minimizar o impacto dos incidentes de segurança da informação de modo a preservar a segurança do patrimônio intangível do IPSEMC.

Resolução Normativa
(Continuação da Resolução 004/13)

Parágrafo Único. Esta resolução não é exaustiva em todas as suas normas de uso e políticas de segurança da informação, ficando de responsabilidade da Comissão propor complementações a alterações sob demanda de novos cenários. A complementação desta resolução sempre deverá ser submetida à equipe previdenciária para a sua devida aprovação tendo em vista o IPSEMC adotar uma gestão participativa e compartilhada.

Art. 3º Esta resolução normativa entrará em vigor na data da sua publicação nos termos deste manual revogando-se as disposições em contrário.

GAPRES, RN Nº 004/2013, de 02 de outubro de 2012.

Certificação Profissional ANBIMA CPA-10

Léa Santana Praxedes
Presidente
lea@ipsemc.pb.gov.br
(83) 3228-4799 / 1434

Prefácio

PREFÁCIO

A gestão pública durante muito tempo agiu à base do amadorismo e isso provocou resultados ineficazes. Hoje, diante das tempestuosas mudanças ocorridas neste mundo globalizado, surge a necessidade de planejar com estratégias de modo a apontar o caminho mais excelente em todas as áreas da organização, inclusive na de Tecnologia da Informação sem a qual ninguém sobrevive, ou seja, normatizar os procedimentos da segurança da informação é um dos pilares essenciais para estabelecer regras claras pois a ausência delas torna as decisões inconsistentes e vulneráveis.

Inicialmente, ocorrem resistências ao estabelecimento de regras e limites para condução das atividades de uma organização pública, entretanto, o nascimento de uma "cultura de segurança da informação" se faz com treinamento, educação e prática até que todos os parceiros, servidores e terceiros incorporem a metodologia e possam descobrir a importância da mesma e entender o porquê de sua adoção.

Assim, no IPSEMC que é um organismo público previdenciário, o principal propósito é proteger o acesso às informações, prevenir inconsistências que possam oferecer riscos às informações institucionais, pois as mesmas servem como base para o desenvolvimento dos processos administrativos necessitando de enquadramento, normatização e melhoria contínua com vistas à proteção do Banco de Dados institucional e a adequação ao que há de mais moderno na área nos últimos tempos.

Este documento está baseado na Estratégia 4 – Programação da Tecnologia da Informação e Comunicação; O.E. 1 – Desenvolver o Projeto de Segurança da Informação do IPSEMC e da Meta 1 – Desenvolver o Projeto de Segurança da Informação do IPSEMC até junho/ 2013 e, como se vê, foi mais um desafio vencido em meio ao turbulento momento de sensível volume de atividades.

Faço questão de registrar os meus agradecimentos sinceros aos professores Ana Lúcia Carvalho de Souza e Arturo Rodrigues Felinto – respectivamente Consultores, à minha irmã Leni S. P. Ribeiro (pela correção dos textos); aos colaboradores incansáveis Jackson Ângelo Pereira (Processamento de Dados), João Thomaz da Silva Neto – Diretor Adm. Financeiro, Carlos Eduardo Toscano Leite Ferreira – Assessor Jurídico, Ítalo Beltrão de Lucena Córdula – Assessor de Informática e Guilhardo de Souza Lourenço – Diretor de Gestão de Investimentos, com os quais este projeto foi construído.

Enfim, meus agradecimentos a DEUS que tem nos propiciado a oportunidade de organizar a gestão pública previdenciária do Município de Cabedelo e sei que estará à nossa frente nos conduzindo à excelência que planejamos.

Minha eterna gratidão!

Léa Santana Praxedes
Presidente – CRA 2723 / CPA 10 ANBIMA

Apresentação

APRESENTAÇÃO

Para o Instituto de Previdência dos Servidores do Município de Cabedelo - IPSEMC a Gestão Estratégica da Informação tem por pressuposto servir como suporte ao alcance da excelência na prestação de seus serviços públicos, notadamente para os Beneficiários do Regime do Próprio de Previdência – RPPS, do Município de Cabedelo, proporcionando uma gestão eficiente dos recursos institucionais e uma melhor troca de informações entre instituições parceiras e fiscalizadoras.

O IPSEMC concentra parte significativa de suas informações em meios digitais, tais como: sites, e-mails e bancos de dados, dentre outros. Atualmente, muitas de suas atividades e processos administrativos a exemplo dos controles de investimentos, financeiros, cadastros de usuários e análises previdenciárias, passou a ser mediada pelas novas tecnologias da informação e comunicação.

Neste contexto, merece destaque ainda o crescente temor por parte das organizações quanto à perda ou violação de seu patrimônio intangível, além da necessidade de garantir aos seus usuários a confidencialidade, a autenticidade, a integridade e a proteção requerida no trato de seus dados e informações.

Este manual representa não apenas um conjunto de normas e diretrizes, padrões e procedimentos a serem adotados no IPSEMC quanto à gestão estratégica de seus recursos informacionais, mas vai além, sendo um guia de boas práticas em tecnologia da informação e segurança para o Instituto.

Apresenta-se o MPSI do IPSEMC distribuído em quatro partes a saber: Parte I (Introdução, Aplicações e Objetivos), Parte II (Comissão de Políticas de Segurança da Informação - CPSI e Controles de Acesso aos Recursos Informacionais), Parte III (Políticas de Segurança da Informação e Parte IV (Boas Práticas, Termos Técnicos e Referências).

O grande desafio aqui apresentado é estimular os servidores e usuários dos serviços do IPSEMC a adoção de uma cultura de boas práticas de tecnologia da informação e comunicação e evidenciar que dessa observância depende, a partir das atitudes das pessoas, o zelo e a proteção ao patrimônio intangível do IPSEMC.

Assim, a relevância no aprimoramento dos controles de gestão e governança aqui abrangidos, visa a garantir a devida proteção da informação e zelar pela integridade dos dados corporativos do IPSEMC enquanto ente do poder público e relacionando-se com suas partes interessadas: sociedade civil, servidores estatutários do município e seus dependentes. Para tanto, a Presidente do IPSEMC, através da Resolução Nº 004/2013/IPSEMC, aprovou este Manual de Políticas de Segurança da Informação.

Ana Lúcia Carvalho de Souza

Arturo Rodrigues Felinto

PARTE I

1.Introdução
2. Aplicações
3. Objetivos

1. INTRODUÇÃO

O estabelecimento de um Manual de Políticas de Segurança da Informação (MPSI) para o IPSEMC, materializado nesse documento, fruto de um projeto maior do Planejamento Estratégico institucional, atende aos anseios de gerenciamento estratégico das informações do Instituto.

Este Manual de Políticas de Segurança da Informação constitui-se num conjunto de diretrizes, normas, padrões e requisitos de segurança no tocante à coleta, ao armazenamento, processamento, manuseio, disseminação e utilização da informação e definição de responsabilidades.

O grande desafio proposto então por esse conjunto de boas práticas é proteger todo o acervo computacional e de informação do IPSEMC contra adulteração, uso indevido, roubo e crimes cometidos por meio digital. Assim, todos que fazem o IPSEMC têm um importante papel a desempenhar para garantir a segurança desses ativos informacionais.

2. APLICAÇÕES

As políticas de segurança da informação de que trata esse manual aplicam-se a todos os servidores, prestadores de serviços, parceiros e usuários que utilizem o ambiente informacional do IPSEMC, ou acesso às informações pertencentes ao Instituto. As políticas de segurança da informação aqui tratadas observam o cumprimento das normas constantes no manual. O descumprimento dessas normas, a exemplo de fraudes e invasão ou violação da integridade dos dados e informações do Instituto, ficará submetido à legislação nacional em vigor.

Aplica-se ainda ao gerenciamento de quaisquer equipamentos, programas, meios físicos de tráfegos e sistemas de armazenamento digital de dados e informações incluindo notebooks, tablets, unidades móveis de armazenamento (discos rígidos-HDs), smartphones, impressoras, além das estações de trabalho, inseridos no ambiente do IPSEMC.

3. OBJETIVOS

O MPSI do IPSEMC atende aos seguintes objetivos:

- Estabelecer as políticas de adoção de softwares livres e outras boas práticas de gestão da informação.
- Estabelecer um quadro global com as responsabilidades da Comissão de Políticas de Segurança da Informação - CPSI do IPSEMC, bem como dos seus colaboradores no que concerne à administração, proteção e uso dos recursos informacionais do Instituto.
- Descrever as políticas de proteção das informações contra acesso não autorizado, manutenção da confidencialidade, integridade e disponibilidade da informação armazenada e assegurar que as medidas legislativas e regulamentares e outros requisitos sejam cumpridos.
- Otimizar o gerenciamento de riscos, prevenir e minimizar o impacto dos incidentes de segurança da informação, de modo a preservar a segurança do patrimônio intangível do IPSEMC.

PARTE II

4. Comissão de Políticas de Segurança da Informação (CPSI)
5. Controles de acesso aos recursos informacionais

4. COMISSÃO DE POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO (CPSI)

4.1 Composição

A Comissão de Políticas de Segurança da Informação (CPSI) do IPSEMC será composta pelo Presidente do IPSEMC, pelo Assessor de Informática Previdenciário, pelo Assessor de Desenvolvimento Institucional e Controle Interno e pelo Chefe do Setor de Processamento de Dados, sendo responsável pela elaboração e aplicação das políticas de segurança da informação do Instituto.

Será formalmente constituída por meio de portaria e a nomeação de seus membros se dará por um período de dois anos, podendo ser renovável. A qualquer momento, por meio de seu Presidente, o IPSEMC pode destituir algum colaborador da CPSI e nomear outro, conforme critérios de segurança adotados pelo Instituto.

4.2 Atribuições e Responsabilidades

Atribuições:

- Estimular a adoção das práticas de segurança da informação preconizadas neste manual, por toda a organização.
- Reunir-se, pelo menos uma vez a cada seis meses, ou extemporaneamente quando houver necessidade.
- Apresentar um relatório formalizando resumidamente e com clareza as ocorrências, deliberações, resoluções e decisões objeto da reunião.

Responsabilidades:

- Definir as políticas constantes neste manual, propor modificações e atualizações quando necessário;
- Orientar os servidores do IPSEMC sobre as políticas e as normas e padrões nele contidos;
- Classificar as informações do IPSEMC;
- Estabelecer os níveis de acesso às informações pelos usuários;
- Criar mecanismos de acesso, controle e monitoramento do uso das informações e meios informacionais;
- Avaliar os incidentes de segurança e propor ações para sua correção;
- Definir as medidas cabíveis nos casos de descumprimento do MPSI, com o auxílio do Assessor Jurídico.

5. CONTROLES DE ACESSO AOS RECURSOS INFORMACIONAIS

O controle de acesso pode ser físico ou lógico e tem como objetivo proteger equipamentos, aplicativos e arquivos do IPSEMC contra perdas, modificações ou violação de seu sigilo. O controle de acesso lógico é um conjunto de procedimentos e medidas com o objetivo de proteger dados, programas e sistemas contra tentativas de acesso não autorizados.

PARTE III

6. Políticas de Segurança da Informação

6. POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO

6.1 Informação: Importância e Classificação

A informação é um ativo intangível de grande valor para as organizações modernas, sendo considerada um fator crítico para seu sucesso e, como tal, requer um tratamento adequado quanto à sua aquisição e/ou produção, armazenamento, disponibilização, uso e proteção.

O acesso às informações proprietárias de uma organização e sensíveis ao seu desenvolvimento, por pessoas não autorizadas e que possam alterá-las ou ainda valerem-se de seu conteúdo para usos particulares outros não contemplados em seu fim precípuo, podem, inclusive, inviabilizar a continuidade das atividades de uma organização.

De acordo com a descrição do item 5.2 da NBR ISO 17799, que versa sobre a classificação da informação:

"O objetivo da Classificação da Informação é assegurar que os ativos da informação recebam um nível adequado de proteção. A informação deve ser classificada para indicar a importância, a prioridade e o nível de proteção. A informação possui vários níveis de sensibilidade e criticidade. Alguns itens podem necessitar um nível adicional de proteção ou tratamento especial. Um sistema de classificação da informação deve ser usado para definir um conjunto apropriado de níveis de proteção e determinar a necessidade de medidas especiais de tratamento".

O MPSI do IPSEMC não se encerra em suas normas aqui estabelecidas quanto à proteção e divulgação de seus recursos informacionais, estando também submetido à Lei nº 12.527 de 18 de novembro de 2011 que dispõe sobre os procedimentos a serem observados pela União, Estados, Distrito Federal e Municípios, com o fim de garantir o acesso à informações previsto no Inciso XXXIII do Art. 5º, no Inciso II do § 3º do Art. 37 e no §2º do Art. 216 da Constituição Federal.

Conforme a NBR ISO/IEC 17799:

> "A informação pode existir de diversas formas. Ela pode ser impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou através de meio eletrônico, mostrada em filmes ou falada em conversas. Seja qual for a forma apresentada ou meio através do qual a informação é compartilhada ou armazenada, é recomendado que seja sempre protegida adequadamente".

A classificação da informação segundo a NBR ISO 17799 adotada pelo IPSEMC é:

- Pública – A informação que pode ser acessada por usuários do IPSEMC, tais como clientes, fornecedores, prestadores de serviços e público em geral.
- Interna – A informação cujo acesso é restrito aos funcionários do IPSEMC, possuindo um nível de confidencialidade que pode comprometer a imagem da instituição.
- Confidencial – A informação que só pode ser acessada por usuários e por parceiros restritos ao IPSEMC.• Restrita – A informação que só pode ser acessada por usuários do IPSEMC explicitamente indicados pelo nome ou por área a que pertence.

Na adaptação da Norma ISSO acima acerca da classificação da informação para o IPSEMC cabe explicitar o termo parceiro como sendo qualquer prestador de serviço e/ou consultor interno ou externo que necessite acessar as informações do Instituto para o desenvolvimento de suas atividades.

A classificação de que trata o item acima é de responsabilidade da CPSI do IPSEMC que deverá analisar a relevância e grau de confi-

dencialidade das informações e documentos do Instituto e atribuir-lhe a escala de prioridade acima.

6.2 Objetivos da Política de Segurança da Informação

A política de segurança da informação visa a garantir a integridade, confidencialidade, autenticidade e disponibilidade das informações processadas pela organização. Veremos abaixo cada um dos termos citados:

a) Integridade – Consiste na conformidade de dados armazenados com relação às inserções, alterações e processamentos autorizados e efetuados.
b) Confidencialidade – Consiste na garantia de que somente pessoas autorizadas tenham acesso às informações armazenadas ou transmitidas por meio de redes de comunicação.
c) Autenticidade – Consiste na garantia da veracidade da fonte das informações.
d) Disponibilidade – Consiste na garantia de que as informações estejam acessíveis às pessoas e aos processos autorizados, a qualquer momento requerido, durante o período acordado entre os gestores da informação e a área de informática.

6.3 Recursos a Serem Protegidos no IPSEMC

A proteção aos recursos informacionais inclui desde aplicativos e arquivos de dados até utilitários além do sistema operacional.

- Aplicativos (programas);
- Arquivos de dados (bases de dados, arquivos ou transações de bancos de dados);
- Arquivos de log (registram quem acessou os recursos informacionais);
- Arquivos de senha; e
- Utilitários e sistema operacional.

6.4 Identificação e Autenticação de Usuários

Os usuários dos sistemas computacionais do IPSEMC são identificados e autenticados durante um processo, chamado logon onde são solicitados a ID (identificação do usuário) e sua senha (autenticação do usuário).

IDENTIFICAÇÃO DO USUÁRIO (ID)

A identificação do usuário, ou ID, deve ser única. Ela permitirá um controle das ações praticadas pelos usuários através dos logs. No IPSEMC a ID adotada será o número do CPF do servidor.

AUTENTICAÇÃO DO USUÁRIO

A primeira senha deverá ser o número da matrícula do servidor. A partir do primeiro acesso ao sistema o usuário deverá alterar a sua senha, por motivos de segurança, customizando-a.
Os usuários dos sistemas informacionais do IPSEMC devem ter pleno conhecimento das políticas de senha da organização, e serem orientados e estimulados a segui-las fielmente. Todos os usuários devem ser solicitados a:

- Manter a confidencialidade das senhas;
- Não compartilhar senhas;
- Estabelecer senhas com tamanho entre seis e oito caracteres;
- Alterar a senha sempre que existir qualquer indicação de possível comprometimento do sistema ou da própria senha;
- Alterar a senha em intervalos de dois meses.
- Alterar a senha para usuários privilegiados (Presidência, Assessorias e Diretorias) a cada dois meses.
- Solicitar, via e-mail, ao Assessor de Informática o cadastro de uma nova senha em caso de esquecimento ou extravio.

Observação:

- O sistema do IPSEMC deve forçar a troca das senhas dos usuários nos períodos estabelecidos lembrando-os a partir do terceiro dia para sua expiração, reforçando o evento da substituição com frases como: “Faltam 2 dias para a sua senha expirar”. (Ex.:Dia “D”-2, “D”-1 e Dia “D”).

6.5 Restrição de Acesso aos Recursos Informacionais

É atribuição da CPSI estabelecer a política de níveis de acesso aos usuários dos sistemas informacionais do IPSEMC, para cada tipo específico de aplicativos, arquivos, informação e/ou documento, imprescindíveis para desempenhar suas funções na organização. Para a definição quanto aos níveis de acesso aos recursos informacionais a Comissão valer-se-á da classificação da informação constante no 6.1.

6.6 Monitoramento do Acesso aos Recursos Informacionais

O monitoramento dos recursos deverá ser realizado pelo Assessor de Informática, de forma contínua, com a elaboração de relatórios das atividades, a serem apresentadas nas reuniões da Comissão, quando necessário.

ACESSO À REDE

Servidores devem solicitar acesso à rede enviando e-mail ao Assessor de Informática do IPSEMC que providenciará o atendimento adequado à solicitação.

INSTALAÇÃO DE PROGRAMAS

O responsável pelo setor que necessitar a instalação de um programa para o desenvolvimento de uma atividade específica deve enviar uma solicitação por e-mail ao Assessor de Informática do IPSEMC que julgará a propriedade da solicitação que vai depender da existência de licenças disponíveis para o programa.

CRIAÇÃO DE E-MAIL

O servidor que necessitar a criação de uma conta de e-mail deve encaminhar a solicitação por escrito, em formulário específico ao Assessor de

Informática do IPSEMC que avaliará a propriedade da solicitação.

A escolha do e-mail corporativo se dará seguindo duas orientações:

1. nome.ultimonome@ipsemc.pb.gov.br
2. setor@ipsemc.pb.gov.br

Casos especiais a exemplo de e-mails homônimos ou outros serão julgados pelo Assessor de Informática do IPSEMC.

ACESSANDO OS SISTEMAS DO IPSEMC

A CPSI estabelecerá os níveis de acesso às informações institucionais. Caso o servidor necessite acessar algum programa específico para o desenvolvimento de suas atividades deve solicitá-lo ao Assessor de Informática do IPSEMC.

Durante o processo de logon na rede o sistema mapeará automaticamente para checar quais os programas que estão habilitados para o setor onde determinado servidor desenvolve suas atividades. Necessidades específicas de acesso às bases de dados do IPSEMC devem ser analisados pelo Assessor de Informática.

POLÍTICA DE BACK-UP

O Assessor de Informática e o Chefe do Setor de Processamento de Dados do IPSEMC são responsáveis pelo estabelecimento das políticas de armazenamento, manutenção de cópias de salvamento e recuperação de dados nos servidores do IPSEMC.

REDES SEM FIO DO IPSEMC

O Assessor de Informática estabelecerá duas redes sem fio (wireless) no âmbito de atuação do IPSEMC. A primeira, aberta aos visitantes do IPSEMC, que devem solicitar a senha com mudança periódica, à recepção do IPSEMC. A segunda, de caráter privado, deve ser compartilhada apenas entre usuários cadastrados no Instituto.

Por razões de segurança, não deverá ser permitido o acesso à rede interna do IPSEMC por meio da tecnologia wireless em computadores e dispositivos móveis pessoais. Para estes, será permitido apenas o acesso à internet como usuário visitante.

CONTROLE DE SENHAS DE ACESSO

O sistema de controle de senhas deve ser configurado para proteger as senhas armazenadas contra uso não autorizado aos sistemas e às redes sem fio do IPSEMC, mantendo-as em arquivos criptografados e estipulando datas de expiração, normalmente recomendado que a troca de senhas seja feita a cada dois meses.

Recomenda-se que, para evitar o uso frequente das mesmas senhas, o sistema de controle mantenha um histórico das últimas senhas utilizadas

por cada usuário.

O Assessor de Informática do IPSEMC deverá desabilitar contas inativas, sem senhas ou com senhas padronizadas.

Deverá haver um procedimento que force a troca de senha imediatamente após a primeira autenticação, quando o usuário poderá escolher a senha que será utilizada dali por diante.

Deverão ser bloqueadas contas de usuários após um determinado número de tentativas de acesso sem sucesso. Atingido esse limite, só a Assessoria de Informática poderá desbloquear a conta do usuário.

6.7 PROCESSO DE IMPLANTAÇÃO DO MPSI

O processo de implantação do Manual de Políticas de Segurança de Informações do IPSEMC é formal devendo, inclusive, melhor se ajustar às necessidades e circunstâncias do ambiente. As principais etapas de implantação bem-sucedida do MPSI são: elaboração, aprovação, implementação, divulgação e manutenção. De forma detalhada veremos abaixo as principais fases que compõem o referido procedimento:

- Identificação dos recursos críticos;
- Classificação das informações;
- Definição dos objetivos de segurança a serem atingidos;
- Análise das necessidades de segurança (identificação das possíveis ameaças, análise de riscos e impactos);
- Apresentação de documento formal à Presidência;
- Aprovação;
- Normatização através de resolução;
- Publicação;
- Divulgação;
- Capacitação de usuários;
- Implementação;
- Avaliação e identificação das mudanças necessárias; e
- Revisão periódica

VERIFICAÇÃO DO COMPUTADOR

A Comissão pode, a qualquer tempo, verificar o conteúdo armazenado no computador de cada usuário.

USO DO COMPUTADOR PORTÁTIL

- Quando o usuário não estiver usando o computador portátil, deve utilizar cabo de proteção física que evita o furto físico do equipamento.
- Caso o computador portátil fique mais de 12 horas sem uso, o usuário deve guardá-lo em um armário com chave.
- Ao transportar o computador portátil no carro, o usuário deve colocá-lo no compartimento porta-malas. O aparelho nunca deve ser deixado em local visível dentro do automóvel.
- Ao viajar com o computador portátil, o usuário deve mantê-lo próximo ao seu corpo e estar atento para evitar furtos em locais públicos.

• O uso de computadores portáteis em locais públicos (aeroportos, recepções de hotéis, restaurantes) deve ser evitado. Caso seja extremamente necessário, o usuário deve tomar todos os cuidados para evitar furto ou perda do equipamento.

RESPONSABILIDADES DO USUÁRIO

O usuário que utiliza os recursos informacionais deve:
• Cuidar adequadamente do equipamento. O usuário é o custodiante destes recursos.
• Garantir a sua integridade física e o seu perfeito funcionamento, seguindo as regras e orientações fornecidas pelo Assessor de Informática e Assessor de Desenvolvimento Institucional e Controle Interno.

INFORMAÇÕES CONTIDAS NO COMPUTADOR

O usuário tem a responsabilidade de transferir para o servidor designado as informações que estão no computador portátil e que precisam possuir cópias de segurança.

OUTRAS PROTEÇÕES

• Deve ser implantada a proteção de tela no computador e/ou proteção de ausência (após um tempo de inatividade, o computador bloqueia o sistema, exigindo senha para ser usado novamente).
• Havendo possibilidade técnica e viabilidade de utilização, pelo Assessor de Informática pode desenvolver e implantar ações para que as informações armazenadas no computador portátil sejam criptografadas, evitando que, em caso de roubo ou perda do equipamento, as informações do IPSEMC sejam acessadas por pessoas não autorizadas.

TERMO DE COMPROMISSO

Para ter acesso à informação do IPSEMC, o usuário deverá assinar (manual ou eletronicamente) um termo de compromisso. Os casos de exceção serão definidos pela Comissão.

QUANTO AO USO DA INTERNET

Autorização
O acesso à Internet através de recursos de tecnologia do IPSEMC necessita ser autorizado pelo Assessor de Informática.

Realização do acesso
• O acesso à Internet somente acontecerá após o usuário se identificar no ambiente de tecnologia do IPSEMC através dos controles do ambiente de rede de computadores.
• O acesso à Internet deve ser feito exclusivamente com os programas (softwares) autorizados e disponibilizados para os usuários pelo Assessor de Informática. O usuário não deve alterar as configurações implantadas nos recursos computacionais que utiliza.

Responsabilidade e forma de uso
O usuário que utiliza o acesso à Internet:
• É responsável por todo acesso realizado com a sua identificação/autenticação.
• Não e permitido acessar locais virtuais (sites) que:
Possam violar direitos de autor, marcas, licenças de programas (softwares) ou patentes existentes.
Possuam conteúdo pornográfico, relacionado a sexo, exploração infantil ou ao crime de pedofilia.
Contenham informações que não colaborem para o alcance dos objetivos do IPSEMC.
Defendam atividades ilegais.
Menosprezem, depreciem ou incitem o preconceito a determinadas classes como sexo, raça, orientação sexual, religião, nacionalidade, local de nascimento ou deficiência física.
Que não tenham relação direta com a atividade profissional desempenhada pelo usuário.
• Não deve retirar (copiar) dos endereços acessados (sites/portais) material que não seja para o uso profissional no IPSEMC. Nesses casos, o usuário deve garantir que está cumprindo a legislação em relação ao direito autoral, licença de uso e patentes existentes e que o uso do material foi autorizado pelo gestor da sua área.
• Não é permitido participar de salas de conversas (*Chat*) *online*, exceto em eventuais situações de uso profissional autorizado pela Presidência e pelo Assessor de Informática.

Uso de serviço de mensagem instantânea
Não é permitido o uso de serviços de mensagem instantânea através dos computadores do IPSEMC, exceto em eventuais situações de uso profissional autorizado pela Comissão e/ou pela Assessoria de Informática.

Uso de serviço de rádio, TV, *download* de vídeos, filmes e músicas
Não é permitido o uso de serviços de rádio, TV, download de vídeos, filmes e músicas, através dos computadores do IPSEMC, exceto em eventuais situações de uso profissional autorizado pela Comissão e/ou pela Assessoria de Informática.

Bloqueio de endereços de Internet
Periodicamente a Assessoria de Informática revisará e bloqueará o acesso para os endereços da Internet que não estejam alinhados com esta Política e com o Código de Ética do IPSEMC.

Uso de Correio Eletrônico particular tipo *WebMail* (centralizado em provedores)
• Os usuários poderão acessar serviços de correio eletrônico particular, tipo *WebMail*, através dos recursos de tecnologia do IPSEMC.
• Esse tipo de acesso está submetido à Política de Segurança da Informação do IPSEMC e aos controles técnicos da Assessoria de Informática.
• Havendo necessidade técnica, esse tipo de acesso poderá ser bloqueado ou suspenso pela Assessoria de Informática.

QUANTO AO USO DO CORREIO ELETRÔNICO (E-MAIL)

Endereço eletrônico do usuário
• O IPSEMC disponibiliza endereços de seu correio eletrônico para utilização do usuário (servidor público ou estagiário) no desempenho de suas funções profissionais. (Ex.:usuario@ipsemc.pb.gov.br)
• O endereço eletrônico disponibilizado para o usuário (empregado ou estagiário) é individual, intransferível e pertence ao Instituto.
• O endereço eletrônico cedido para o usuário (servidor público ou estagiário) deve ser o mesmo durante todo o seu período de vínculo com O IPSEMC. Se houver necessidade de troca de endereço, a alteração deverá ser autorizada pela Assessoria de Informática e registrada para possibilitar uma posterior verificação de autoria.

Criação, manutenção e exclusão do endereço de correio eletrônico
• A utilização desse endereço de correio eletrônico pelo usuário (servidor público ou estagiário) necessita ser autorizada pela Assessoria de Informática.
• A liberação do endereço de correio eletrônico será feita pela Assessoria de Informática de maneira controlada e segura.
• Em caso de desligamento ou férias do usuário (servidor público ou estagiário), via de regra, a senha deve ser bloqueada pela Assessoria de Informática.
• No retorno da(s) licença ou férias o usuário (servidor público ou estagiário) deve entrar em contato com a Assessoria de Informática para solicitar o desbloqueio da senha, gerando assim mais segurança para o sistema.

Endereço eletrônico de programas ou de comunicação corporativa
• É permitido que um programa aplicativo ou um programa de sistema possua um endereço de correio eletrônico.
Nesse caso, é obrigatória a existência de um usuário da ATI responsável por acompanhar as mensagens emitidas e recebidas por esse endereço.

Acesso à distância
• O usuário (servidor público ou estagiário) pode acessar o seu endereço eletrônico cedido pelo IPSEMC mesmo quando estiver fora do ambiente do Instituto.

Envio e recebimento de mensagens
• O endereço eletrônico de usuário do tipo prestador de serviço ou estagiário somente poderá enviar e receber mensagens de endereços de coreio eletrônico do IPSEMC.
• O endereço eletrônico dos demais tipos de usuário pode enviar e receber mensagens internas ou externas.

Propriedades do endereço
• O endereço de correio eletrônico disponibilizado para o usuário e as mensagens associadas a esse endereço são de propriedade da (servidor público ou estagiário).
• Em situações autorizadas pela Presidência, as mensagens do correio eletrônico de um usuário poderão ser acessadas, em casos especiais, a critério d CPSI.

Responsabilidades e forma de uso
O usuário que utiliza um endereço de correio eletrônico:
• É responsável por todo acesso, conteúdo de mensagens e uso relativos ao seu e-mail.
• Pode enviar mensagens necessárias para o seu desempenho profissional no Instituto.
• Não é permitido criar, copiar ou encaminhar mensagens ou imagens que: contenham declarações difamatórias ou linguagem ofensiva; façam parte de correntes de mensagens, independentemente de serem legais ou não e repassem propagandas ou mensagens de alerta sobre qualquer assunto.

PARTE IV

7. Boas Práticas
8. Termos úteis

7. BOAS PRÁTICAS

. Utilize senhas fortes, com 8 (oito) ou mais caracteres e as altere periodicamente.
. Utilize um bom antivírus e antispyware/malware.
. Utilize criptografia nos diretórios onde há informações sensíveis.
. Tome cuidado com downloads e com e-mails de remetentes desconhecidos.
. Sempre armazene seus dados em um disco externo (preferencialmente com opção de criptografia).
. Somente acesse endereços de sites confiáveis, verificando se o link demonstrado é realmente o link que o endereço está sendo apontado.
. Ao entrar num site/portal, sempre verifique se todos os links funcionam corretamente. Pois, muitos fraudadores lançam mão de páginas reais para fazer uma cópia.
. Remova e-mails que chegam para você com propagandas não solicitadas para evitar alguma possível contaminação.
. Utilizar *software* originais ou livres.

8. TERMOS ÚTEIS

. Anexos de email – Arquivos enviados no formato digital por email.
. Backup- Cópia de segurança de arquivos.
. Criptografia da Informação - É um processo matemático que transforma a informação original em uma sequência de dados ilegíveis, garantindo a sua confidencialidade, e depois permite retornar à informação original (legível).
. Download - Descarregamento, transferência de arquivos entre computadores por meio de uma rede.
. Hacker - Pessoa que tenta acessar sistemas sem autorização, usando técnicas próprias ou não, no intuito de ter acesso a determinado ambiente para proveito próprio ou de terceiros.
. Log - O log é um registro cronológico de atividade do sistema que possibilita a reconstrução, revisão e análise do ambiente e das atividades relativas a uma operação.
. Login - Registro do histórico de atividades realizadas ou de eventos ocorridos em um determinado sistema ou processo.
. Logon - Processo de identificação e autenticação de um usuário para permitir o seu acesso a um sistema.
. NBR ISO 17799 - Norma da Associação Brasileira de Normas Técnicas (ABNT) trata de técnicas de segurança em Tecnologia da Informação e funciona como um código de prática para a gestão da segurança da informação.
. Redes sem fio (*Wireless*) - É uma rede que pode ser acessada sem a necessidade de conexões por fios.
. Scanners - periférico de digitalização de imagens e documentos.
. Spyware - Software que coleta informações de internautas sem o conhecimento das vítimas.

9. REFERÊNCIAS

Associação Brasileira de Normas Técnicas. **NBR ISO/IEC 27001 - Tecnologia da informação** — Técnicas de segurança — Sistemas de gestão de segurança da informação — Requisitos. Rio de janeiro: ABNT, 2006.

Associação Brasileira de Normas Técnicas. **ABNT NBR ISO/IEC 27002 - Tecnologia da informação** - Técnicas de segurança - Código de prática para a gestão de segurança da informação. Rio de Janeiro: ABNT, 2005.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 17799** - **Tecnologia da informação**: Código de prática para a gestão da segurança da informação. Rio de Janeiro: ABNT, 2001.

BRASIL. Tribunal de Contas da União. **Boas Práticas em Segurança da Informação.** 2 ed. Brasília: TCU, Secretaria de Fiscalização de Tecnologia da Informação, 2007.

_____.Constituição (1988). **Constituição da República Federativa do Brasil de 1988**. Disponível em: <http://www.planalto.gov.br/ccivil_03/Constituicao/Constituiçao. htm>. Acesso em: 20 fev. 2013.

_____. **Decreto no 3.505, de 13 de junho de 2000**. Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal. Disponível em: <www.planalto.gov.br/ccivil_03/decreto/d3505.htm>. Acesso em: 16 mar. 2013.

CASTRO, Maria Alice Soares de. **Guia de Boas Maneiras na Internet**. Nova Editora, 1997. Trechos disponíveis em <http://www.icmc.usp.br/manuals/BigDummy/netiqueta.html>. Acesso em: 13 fev. 2013.

DIAS, Cláudia. **Segurança e auditoria da tecnologia da informação**. Rio de Janeiro: Axcel Books, 2000.

FULGÊNCIO, Paulo Cesar. **Glossário Vade Mecum**. Rio de Janeiro: Mauad Editora Ltda., 2007.

Netiqueta. Disponível em <http://pt.wikipedia.org/wiki/Netiqueta>. Acesso em: 15 fev. 2013.

SANTOS, Daniel. **O quem é quem das pragas virtuais**. Disponível em: <http://pcworld.uol.com.br/> Acesso em: 28 mar. 2013.

IPSEMC

Instituto de Previdência dos Servidores Municipais de Cabedelo

R. Juarez Távora, 648 - Praia Formosa - Cabedelo-PB - CEP: 58310-000

Tels.: +55 83 3228.4799 / 3228.1434 email: ipsemc@ipsemc.pb.gov.br

www. ipsemc.pb.gov.br facebook.com/ipsemc

Manual de Políticas de Segurança da Informação

Instituto de Previdência dos
Servidores Municipais de Cabedelo
IPSEMC