MANUAL DE NORMAS E PROCEDIMENTOS DE CONTROLE DE ACESSO FÍSICO E LÓGICO

IPSEMC
Instituto de Previdência dos Servidores Municipais de Cabedelo
VALORIZANDO O SEU FUTURO

SUMÁRIO

1. OBJETIVO DO MANUAL

Sistematizar o processo de **Controle de Acesso Físico e Lógico** no âmbito do Instituto de Previdência dos Servidores Municipais de Cabedelo – IPSEMC, determinar as responsabilidades dos envolvidos neste processo, bem como descrever como deve ser executado, assegurando desta forma a padronização de execução, desempenho e qualidade do procedimento.

2. LEGISLAÇÃO APLICADA E/ OU DOCUMENTOS COMPLEMENTARES

2.1 Lei 687/93**.**

2.2 Planejamento Estratégico do IPSEMC – Estratégia 3 - Programação de Tecnologia da Informação e Comunicação.

2.3 Portaria nº 185/2015 atualizada pela Portaria SPREV nº 4.248, de 22 de dezembro de 2022, publicada no DOU do dia 23/12/2022, com vigência a partir de 02 de janeiro de 2023, Manual do Pró Gestão RPPS – Versão 3.5.

2.4 Política de Segurança da Informação – PPSI.

2.5 Plano de Contingências dentro da Política de Segurança da Informação do IPSEMC.

2.6 Portaria Ministerial nº 1.467/2022 - Disciplina também os parâmetros e as diretrizes gerais para organização e funcionamento dos regimes próprios de previdência social dos servidores públicos da União, dos Estados, do Distrito Federal e dos Municípios, em cumprimento à Lei nº 9.717, de 1998, aos Arts. 1º e 2º da Lei nº 10.887, de 2004 e à Emenda Constitucional nº 103, de 2019.

2.7 Código de Ética do IPSEMC disposto no Portal: www.ipsemc.pb.gov.br no link: http://www.ipsemc.pb.gov.br/pg16/codigodeetica.aspx

3. RESPONSABILIDADES

Quem participa	Responsabilidades
Setor de Recepção e Protocolo	Recepciona pessoas e/ou documentos, registra, encaminha
Assessoria de Informática - ASSINFOR	Elabora, encaminha, controla o cumprimento / andamento.
Setor de Processamento de Dados	Elabora, encaminha, controla o cumprimento / andamento.
Comissão de Política de Segurança da Informação	Elabora, encaminha, controla o cumprimento / andamento.
Assessoria de Controle Interno	Emite a declaração de conformidade.
Diretoria Executiva - DE	Recebe analisa / Delibera / Autoriza.
Assessoria Jurídica	Analisa e oferta parecer em caso de necessidade.

4. INTRODUÇÃO

O IPSEMC é certificado em Nível III no Programa Pró-Gestão RPPS, coordenado pela Secretaria de Previdência Social - SPREV, do Ministério do Trabalho e Previdência Social – MTPS por meio do qual implementou-se o mapeamento das áreas de atuação e a manualização dos procedimentos da Autarquia colocando-a nesse padrão de excelência pública.

Enquadrar-se em um padrão de excelência pública sempre foi nosso foco principal face a enorme responsabilidade que assumimos, razão porque temos que exercer a missão com austeridade, ética e transparência na gestão pública. Como parte integrante dessa mudança e modernização foi elaborado este ***Manual de Normas e Procedimentos de Controle de Acesso Físico e Lógico*** para padronizar, organizar e melhorar o fluxo de cumprimento visando uma gestão mais eficiente do processo.

O avanço tecnológico tem permitido melhoria dos controles apesar de suas muitas implicações, entretanto a cada dia as rotinas administrativas são atreladas aos instrumentos de tecnologia da informação, sejam eles no sentindo físico, naquilo que se refere a equipamentos e máquinas, bem como ao ambiente virtual onde as atividades são desenvolvidas, visto que com a adoção de RPPS Digital os fatores tecnológicos tomaram proporção geral e se tornaram imprescindíveis nas atividades funcionais do RPP.

Para que se obtenha resultado eficaz o presente *Manual* tem por objetivo regulamentar, informar e orientar sobre a instrução processual do processo de controle de acesso físico e lógico do IPSEMC nos termos da legislação pertinente em vigor e assim facilitar o desenvolvimento da atividade por meio do esclarecimento das normas aplicadas, dos conceitos básicos aqui contidos, mapeamento do processo da atividade, contribuindo assim para a otimização e transparência da atividade do setor de tecnologia da informação.

Este Manual está sempre sujeito a novas alterações desde que sejam necessárias uma vez que a gestão previdenciária é muito dinâmica. Geralmente, ocorrem adventos de novos dispositivos legais publicados, ficando o setor responsável pelas atualizações sempre que for preciso.

Os manuais do IPSEMC são frutos de um trabalho intensivo e exaustivo dedicado a esclarecer a execução das ações, dos processos e atividades em geral, como também para facilitar a compreensão de todos os operadores do sistema uma vez que apresenta o passo-a-passo de forma clara e inequívoca.

Ressalta-se que esta publicação é produto do novo modelo de Governança adotado pelo IPSEMC em nível do Pró-Gestão RPPS, focado na valorização dos servidores, na excelência da atividade pública, no estímulo ao desenvolvimento das competências de sua força de trabalho e na potencialização do capital humano do Instituto que é o nosso patrimônio maior.

Façam um bom uso deste Manual realizando um ótimo trabalho.

Léa Santana Praxedes
Presidente

5. DEFINIÇÃO DE PLANO DE CONTINGÊNCIAS

Segundo o Plano de Contingências do IPSEMC, estabelecido por meio da Resolução Normativa – RN nº 08/2020 é: "um planejamento de riscos que tem o objetivo de descrever as medidas a serem tomadas por uma empresa, incluindo a ativação de processos manuais, para fazer com que seus processos vitais voltem a funcionar plenamente, ou num estado minimamente aceitável, o mais rápido possível, evitando assim uma paralisação prolongada que possa gerar maiores prejuízos a corporação".

No caso de um RPPS, pode-se observar, a princípio, a necessiades de preparar-se para eliminar ou mitigar riscos que possam advir de:

- ✓ Perdas de receita;
- ✓ Perdas nos investimentos;
- ✓ Sanções governamentais;
- ✓ Problemas jurídicos para os dirigentes;
- ✓ Abordagens maliciosas seja de onde vier;
- ✓ Comportamentos de servidores;
- ✓ Acesso de servidores e segurados em todos os âmbitos.

6. CONCEITOS E/OU OUTRAS DEFINIÇÕES BÁSICAS

6.1 Previdência Social

É um programa do Governo que consiste em uma forma de seguro que oferece proteção a todo cidadão contribuinte contra diversos riscos como doença, invalidez, morte e velhice.

6.2 Regime Geral de Previdência Social – RGPS

É o conjunto de regras que estabelecem os direitos e deveres relacionados ao sistema previdenciário do Brasil, garantindo os direitos assistenciais à população.

6.3 Regime Próprio de Previdência Social – RPPS

Regime previdenciário próprio de cada ente federativo, de filiação obrigatória para os servidores públicos titulares de cargo efetivo.

6.4 Acesso

Ato de ingressar, transitar, conhecer ou consultar a informação, seja local, ou remotamente, bem como a possibilidade de usar os ativos de informação de um órgão ou entidade.

6.5 Área Segura

São ambientes ou salas trancadas ou ainda um conjunto de salas dentro de um perímetro físico de segurança, que podem ser trancados, pois pode conter arquivos de aço trancáveis, fichários e ou outros armários e equipamentos. Sendo assim, a localização de uma área segura deve levar em conta os riscos e vulnerabilidades e devem contemplar os regulamentos e normas relevantes de saúde e segurança e considerar eventuais ameaças à segurança causadas por instalações vizinhas, como infiltrações, vazamento de água ou outros eventuais problemas.

6.6 Ativos de Informação

Os meios de armazenamento, transmissão e processamento da informação; os equipamentos necessários a isso; os sistemas utilizados para tal; os locais onde se encontram esses meios, e também os recursos humanos que a eles têm acesso.

6.7 Bloqueio de Acesso

Processo que tem por finalidade suspender temporariamente o acesso.

6.8 Contas de Serviço

Contas de acesso à rede coorporativa de computadores necessária a um procedimento automático (aplicação, script etc.) sem qualquer intervenção humana no seu uso.

6.9 Credenciamento de Acesso

Processo pelo qual o usuário recebe credenciais que concederão o acesso, incluindo a identificação, a autenticação, o cadastramento de código de identificação e definição de perfil de acesso em função de autorização prévia.

6.10 Credenciais ou Contas de Acesso

Identificações concedidas por autoridade competente após o processo de credenciamento de acesso, que permitam habilitar determinada pessoa, sistema ou organização ao acesso. A credencial pode ser física, como crachá, cartão, credencial biométrica, pulseira ou lógica como identificação de usuário e senha.

6.11 Contêineres dos Ativos de Informação

O contêiner é o local onde "vive" o ativo de informação, onde está armazenado, como é transportado ou processado.

6.12 Custodiante do ativo de informação

É o responsável pelos contêineres dos ativos de informação e pela aplicação dos níveis de controles de segurança em conformidade com as exigências de segurança da informação e comunicações, comunicadas pelos proprietários dos ativos de informação.

6.13 Equipamentos

Instrumentos necessários para determinada função.

6.14 Exclusão de Direito de Acesso

Processo que tem por finalidade suspender definitivamente o acesso.

6.15 Exclusão de Conta de Acesso

Processo que tem por finalidade o cancelamento do código de identificação e do perfil de acesso.

6.16 Gestão de Riscos 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.

6.17 Gestor do ativo de informação

Indivíduo legalmente instituído por sua posição e/ou cargo, o qual é responsável primário pela viabilidade e sobrevivência dos ativos de informação.

6.18 Identificação do Usuário ou Nome do Usuário

Forma pela qual o usuário é conhecido no ambiente de informática do IPSEMC. O usuário recebe as permissões de utilização dos recursos computacionais em função de sua Identificação, que deve ser validada com o uso de uma Senha.

6.19 Menu

Lista de opções ou entradas postas à disposição do usuário, que aparece no vídeo de um terminal de computador com as funções que este poderá realizar por meio de um programa ou de um software.

6.20 Necessidade de Conhecer

Condição pessoal, inerente ao efetivo exercício de cargo, função, emprego ou atividade, indispensável para o usuário ter acesso à informação, especialmente se for sigilosa, bem como o acesso aos ativos de informação.

6.21 Perfil de Acesso

Conjunto de atributos de cada usuário, definidos previamente como necessários para credencial de acesso.

6.22 Perímetro de Segurança

Áreas que podem ser compostas por diferentes dimensões, equipamentos e tipos de controle de acesso físico para as instalações ou áreas críticas. Podem ser delimitadas por paredes, portas de entrada controladas por cartão ou balcão de recepção com recepcionista, etc.

6.23 Quebra de Segurança

Ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e comunicações.

6.24 Tratamento da Informação

Recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação, inclusive as sigilosas.

6.25 Usuário

Qualquer servidor ocupante de cargo efetivo, cargo em comissão, cedido, prestador de serviço terceirizado, estagiário ou qualquer outro indivíduo que tenha acesso, de forma autorizada, aos recursos computacionais do IPSEMC.

6.26 Periódico Oficial do IPSEMC – POI

Veículo de comunicação entre os órgãos públicos e a sociedade, que tem por objetivo tornar público todo e qualquer ato acerca da Administração Previdenciária do IPSEMC.

7. FINALIDADE DA ASSESSORIA DE INFORMÁTICA PREVIDENCIÁRIA

De forma geral e abrangente, a Assessoria de Informática Previdenciária é o órgão responsável por gerir as atividades relacionadas à gestão de Tecnologia da Informação do Instituto de Previdência dos Servidores de Cabedelo – IPSEMC, conjuntamente com o Setor de Processamento de Dados em conjunto com a Comissão de Política de Segurança da Informação, incluso o processo de elaboração de planos de controle de acesso físico e lógico.

8. ÓRGÃOS DE RELACIONAMENTO INSTITUCIONAL VINCULADOS

8.1 Assessoria de Informática
8.2 Setor de Processamento de Dados
8.3 Assessoria de Controle Interno
8.4 Assessoria Jurídica
8.5 Presidência
8.6 Setores do IPSEMC.

9. DETALHAMENTO DO PROCESSO

MANUALIZAÇÃO DO PROCESSO DE CONTROLE DE ACESSO FÍSICO E LÓGICO				
	ETAPA/ATIVIDADE	**DETALHAMENTO DAS ROTINAS E PROCEDIMENTOS A SEREM SEGUIDOS**	**INDICADOR DE DESEMPENHO**	**CONTROLES DA ATIVIDADE**
1	**SEPROD** **Setor de Recepção e Protocolo** I- Pessoas II- Documentos	✓ O colaborador do atendimento deverá **Recepcionar** pessoas (clientes / usuários) ✓ Procurar se inteirar para qual setor se destina ✓ Registrar no Livro de Controle de Acesso conforme estabelecido autorizando ou não a entrada ✓ Encaminhar ao Setor competente ✓ Monitorar e Acompanhar o Acesso Físico. ✓ Quanto a documentos, Receber, registrar e encaminhar ao Setor competente ✓ Fornecer WI FI só o de visitantes caso seja solicitado	Conforme definido no Planejamento Estratégico	Lei 687/93. Planejamento Estratégico do IPSEMC – Estratégia 3 - Programação de Tecnologia da Informação e Comunicação. Portaria nº 185/2015 atualizada pela Portaria SPREV nº 4.248, de 22 de dezembro de 2022, publicada no DOU do dia 23/12/2022, com vigência a partir de 02 de janeiro de 2023., Manual do Pró Gestão RPPS – Versão 3.4. Política de Segurança da Informação – PPSI. Plano de Contingências dentro da Política de Segurança da Informação do IPSEMC. Portaria Ministerial nº 1.467/2022 - Disciplina também os parâmetros e as diretrizes gerais para organização e funcionamento dos regimes próprios de previdência social dos servidores públicos da União, dos Estados, do Distrito Federal e dos Municípios, em
2	**Prestadores de Serviços / Aposentados / Clientes Usuários / Beneficiários – Segurados / Fornecedores** ✓ Pessoas	1- Cumprir com os registros e autorizações de entrada e saída 2- Utilizar acesso lógico somente mediante autorização 3- Fornecer contato, e-mail, endereço para envio da Política de Segurança da Informação e do Código de Ética (se for o caso.)		
3	**Setor Competente (Gabinete da Presidência e/ou setores do Instituto)** I- Documentos **II-** Pessoas	✓ Se for documento, analisar e dar os encaminhamentos devidos. ✓ Se for pessoas, confirmar o registro e autorizar ou não a entrada ✓ Receber / atender		

4	**ASSINFOR** **Assessoria de Informática** **SEPROD** **Setor de Processamento de Dados** I- Computadores Institucionais II- Estabelecer senhas de acesso	✓ Estabelecer junto com cada colaborador a senha de acesso individual da máquina na qual opera ✓ Orientar o servidor a criar sua própria senha e memorizar porque o acesso é individual ✓ Monitorar		cumprimento à Lei nº 9.717, de 1998, aos Arts. 1º e 2º da Lei nº 10.887, de 2004 e à Emenda Constitucional nº 103, de 2019. Código de Ética do IPSEMC
5	**Colaboradores / Servidores do Instituto** I- Computadores Institucionais II- Criar senhas de acesso III- E-mail institucional IV- Outros documentos	✓ Criar sua senha de acesso ✓ Utilizar / Acessar conforme regras estabelecidas ✓ Acompanhar / Comunicar e Registrar Ocorrências. ✓ Fazer os encaminhamentos que vierem a necessitar de soluções e respostas. ✓ Monitorar / Acompanhar o resultado ✓ Registar também a saída de documentos, verificar se foi entregue. ✓ Verificar de existem pendências ✓ Colaborar com as respostas / soluções ✓ Participar dos treinamentos e capacitações visando a melhoria contínua do serviço público que presta, bem como dos controles utilizados pela Autarquia. ✓ Capacitar-se, dar o seu melhor.		

10. GESTÃO DE RISCOS

A Gestão de riscos é um tema de alta relevância para qualquer negócio e, por isso, nossa Autarquia tem demonstrado muita preocupação frente aos obstáculos que nos surge seja no ambiente interno, seja no externo. Os riscos são importantes para as decisões estratégicas e a principal causa de incertezas dos processos no âmbito das organizações. Além disso, estão presentes nas atividades mais simples que se realiza. Por mais que entendamos que a gestão de risco envolve uma abordagem ampla e corporativa, admitimos de forma clara e objetiva neste documento os pontos que julgamos necessários para que sejam observados pelo setor, por entendermos que permite um cuidado e uma organização parametrizada na legislação vigente como também que o IPSEMC contabilize o potencial impacto que produzirá nos processos, atividades e serviços que presta aos segurados, à sociedade. Neste caso, destacamos:

I- Risco Legal

Envolve qualquer infração às leis que possam ser cometidas, de forma consciente ou não. Quando ocorre ausência de documentos obrigatórios; ferramentas equivocadas ou outro evento que deverá fazer parte do processo. Neste caso, deverá ser feita uma Notificação por parte dos responsáveis e encaminhado para o setor correspondente dando prazo para sanar as pendências.

Havendo a devida conferência e correção todo o processo deverá estar em conformidade com a legislação vigente em todos os aspectos. Permanecer sempre com a legislação que rege a matéria atualizada, atentando sempre para os aspectos legais.

II- Risco Operacional

Representa as perdas geradas por eventos internos da rotina do setor, como falhas de funcionários, de sistemas, equipamentos. Para evitá-lo, algumas iniciativas devem ser tomadas, como observância junto à mesa de trabalho para ver se há ação a ser executada, comunicar ao setor que esteja parado ou não tenha observado sua mesa de trabalho, agir com proatividade e eficiência para gerar resultado eficaz.

III- Risco Reputacional

Representa todos os eventos internos ou externos com capacidade de manchar ou danificar a percepção do IPSEMC perante a mídia, os colaboradores, os segurados e a sociedade em geral. Deve-se sempre preocupar-se com uma conduta respeitável, honesta, transparente, pautada numa postura ética, lembrando que o comportamento condenável pode ser registrado e divulgado o que pode colocar toda nossa reputação a perder. Neste caso, observar sempre o que dispõe o nosso Código de Ética.

11. DISPOSIÇÕES FINAIS

A execução da gestão do processo de Controle de Acesso Físico e Lógico do IPSEMC deve seguir o método descrito neste Manual Normativo cujas etapas estão estabelecidas e padronizadas, necessariamente, respeitando a ordem da sua descrição, estando sempre sujeitas a alterações e melhorias no sentido de promover-se ajustes com o fito de otimizar os procedimentos e maximizar os resultados uma vez que procedimentos de verificação e compliance auxilia no monitoramento das atividades operacionais e administrativas para cumprimento da missão institucional.

A competência para a proposição de alterações neste Manual de Normas e Procedimentos do processo de Controle de Acesso Físico e Lógico é da Assessoria de Informática Previdenciária, do Setor de Processamento de Dados, como também da Comissão de Política de Segurança da Informação que, detectando a necessidade de atualização ou ajustes, afere junto ao próprio Setor e apresenta à Diretoria Executiva para deliberação final.

Diante do exposto, as etapas dos procedimentos de **Controle de Acesso Físico e Lógico** serão executadas, necessariamente, respeitando-se a ordem descrita neste Manual Normativo.

REFERÊNCIAS

Guia para elaboração de plano de contingência metodologia CELEPAR. Ano de edição: Agosto 2009. Guia para elaboração de plano de contingência metodologia CELEPAR.

https://pt.wikipedia.org/wiki/Plano_de_conting%C3%AAncia#:~:text=Os%20procedimentos%20mais%20simples%20de,%2C%20por%20exemplo)%2C%20ter%20c%C3%B3pias

https://blogdaqualidade.com.br/como-elaborar-um-plano-de-contingencia/

APROVADO PELA DIRETORIA EXECUTIVA EM CONFORMIDADE COM O CONTROLE INTERNO		
JOÃO THOMAZ DA SILVA NETO Diretor Administrativo Financeiro Membro	**LÉA SANTANA PRAXEDES** Presidente	**GUILHARDO DE SOUSA LOURENÇO** Diretor de Gestão de Investimentos Membro
DARCIO XAVIER FERREIRA Assessor de Des. Inst. e Controle Interno		