

	Instituto de Previdência do Município de Cachoeiro de Itapemirim Estado do Espírito Santo	NORMA DE PROCEDIMENTO	SADM-NP 002/2019
Assunto:			
PROCEDIMENTOS DE CONTINGÊNCIA DE DADOS E CONTROLE DE ACESSOS FÍSICO E LÓGICO			
Versão: 02	Data de elaboração: 30/09/2019	Data da aprovação: 07/12/2022	Data de vigência: 07/12/2022
Ato de aprovação: Portaria nº 148/2022		Unidade Responsável: Diretoria Administrativa	
Revisada em: 05/12/2022		Revisado por: Coordenador de Área – Tecnologia da Informação	
Anexos: Anexo I – Fluxograma Cópia de Segurança de Servidor de Arquivo e Sistemas de Informações Automatizados Anexo II – Fluxograma Políticas de Controle de Acesso Lógico Anexo III – Fluxograma Controle de Acesso Físico ao Ambiente Tecnológico do IPACI			
Aprovação:			
<i>Assinatura da Diretora Administrativa</i>		<i>Assinatura da Coordenadora Executiva de Controle Interno</i>	
<i>Assinatura da Presidência Executiva</i>			

1. Finalidade:

Definir procedimentos para realização de cópias de segurança dos sistemas informatizados e dos bancos de dados e procedimentos de controle de acesso físico e lógico.

2. Abrangência:

Todas as unidades executoras do Instituto.

3. Base Legal e Regulamentar:

Política de Segurança da Informação
Decreto Municipal nº 30.492/2021

4. Conceitos:

Alfanuméricas: combinação de letras e números;

Backup: cópias de segurança de arquivos com o objetivo de restaurá-los no menor tempo possível caso haja necessidade;



Helpdesk: termo em inglês que significa literalmente "balcão de ajuda" e que se refere a um serviço de atendimento remoto aos clientes que procuram por soluções, esclarecimentos sobre dúvidas e outras solicitações para problemas técnicos relacionados a informática ou tecnologia da informação.

Logar: Ter acesso à área reservada de um site ou programa de computador através de um login de usuário ou senha;

Reset: restauração para seu estado primário, ou em melhor estado;

Servidor de arquivo: é um servidor dedicado que tem o objetivo principal de proporcionar um local para o armazenamento compartilhado de arquivos de computadores que podem ser acessados por outras estações trabalho que estão ligados à rede do mesmo.

Tecnologia da informação: conjunto de recursos tecnológicos e computacionais para geração e uso da informação, abrangendo todas as atividades desenvolvidas na sociedade pelos recursos da informática;

Unidade Executora: diversas unidades da estrutura organizacional que se sujeitam à observância das rotinas de trabalho e dos procedimentos de controle estabelecidos na Norma de Procedimento;

5. Competências e Responsabilidades:

5.1 – Coordenadoria de Área – Tecnologia da Informação (IPACI)

5.1.1 – Proceder com o controle, manutenção, restauração e operacionalização dos dados solicitados;

5.1.2 – Alertar todos os colaboradores sobre eventuais manutenções que possam ocasionar perda de dados;

5.1.3 – Controlar acesso físico de usuários externos e prestadores de serviços às dependências do Ambiente Tecnológico do Instituto;

5.1.4 – Cumprir fielmente as determinações da Norma de Procedimentos, em especial quanto aos procedimentos na geração de documentos, dados e informações.

5.2 – Usuários

5.2.1 – Logar os sistemas e contas de e-mail, em cada acesso, sendo vedado manter login e senhas salvos automaticamente;

5.2.2 – Bloquear sua estação de trabalho sempre que se ausentar do ambiente de trabalho.

5.3 – Coordenadoria de Tecnologia da Informação – CTI (PMCI)

5.3.1 – Coordenar ações de Segurança da Informação e Proteção de Dados Pessoais;

5.3.2 – Estruturar uma política de backup de todos os sistemas e arquivos armazenados no DATACENTER da administração direta e indireta do Município de Cachoeiro de Itapemirim;

5.3.3 – Permitir acesso lógico aos usuários interno e externo do Instituto;

5.4 – Presidência Executiva

5.4.1 – Solicitar a criação/atualização de contas de acesso lógico à CTI e de Prestadores de Serviço de Sistema de Informação Automatizado.



5.5 – Prestadores de Serviço

5.4.1 – Desempenhar suas funções conforme ditames contratuais.

5.5 – Coordenadoria Executiva do Controle Interno – CECI

5.5.1 – Prestar apoio técnico e avaliar a eficiência dos procedimentos de controle inerentes a presente Norma de Procedimento.

6. Procedimentos:

CÓPIAS DE SEGURANÇA SERVIDOR DE ARQUIVOS

6.1 – Usuários

6.1.1 – Armazenar dados no servidor de arquivos do Instituto;

6.2 – Coordenadoria de Tecnologia da Informação – CTI (PMCI)

6.2.1 – Realizar diária, semanal e mensalmente rotinas de backups nos servidores da PMCI, nos moldes da política de backup relacionado no arts. 55 e 56 do Decreto Municipal nº 30.492/2021;

6.3 – Usuários

6.3.1 – Comunicar através de e-mail à Coordenadoria de Área de Tecnologia da Informação do Instituto a perda de dado(s), constante(s) no *servidor de arquivo*, contemplado pela rotina de backup, informando nome, local e data da última modificação do arquivo;

6.4 – Coordenador de Área – Tecnologia da Informação (IPACI)

6.4.1 – Solicitar restauração dos dados através do serviço Helpdesk disponibilizado pela PMCI por meio abertura de chamado por meio de telefone, e-mail ou site para abertura do chamado;

6.5 – Coordenadoria de Tecnologia da Informação - CTI

6.5.1 – Analisar os dados informados no chamado quanto ao nome, local e data da última modificação do arquivo;

6.5.1.1 – Identificando o arquivo informado, restaura-o, disponibilizando uma cópia na pasta “restore” localizada no servidor de arquivos;

6.5.1.2 – Não identificando o arquivo, informar ao usuário os motivos e encerrar o chamado;

6.6 – Coordenador de Área – Tecnologia da Informação (IPACI)

6.6.1 – Informar ao usuário quanto a restauração ou não do arquivo solicitado;

6.7 – Usuários

6.7.1 – Utilizar o arquivo/informação nos termos da Política de segurança da Informação e Decreto Municipal nº 30.492/2021.



CÓPIAS DE SEGURANÇA SISTEMAS DE INFORMAÇÕES AUTOMATIZADOS

6.8 – Usuários

6.8.1 – Inserir / acessar as informações relacionadas a cada área de atuação nos sistemas de informações automatizados, contratados para realizar a gestão da informação do Instituto;

6.9 – Prestador de Serviço de Sistema de Informação Automatizado

6.9.1 – Realizar rotina de backup nos termos contratuais de cada prestador de serviço/locador;

6.10 – Usuários

6.10.1 – Cientificar à Coordenador de Área – Tecnologia da Informação (IPACI) e comunicar ao fiscal do contrato, através de e-mail, a perda de dado(s), constante(s) no sistema de informação automatizado, informando os dados perdidos e a data da última modificação;

6.11 – Coordenador de Área – Tecnologia da Informação (IPACI) / Fiscal de Contrato

6.11.1 – Solicitar restauração dos dados através de chamado à empresa terceirizada por meio de chamado, telefone ou e-mail;

6.12 – Prestador de serviço de Sistema de Informação Automatizado

6.12.1 – Restaurar os dados solicitados e disponibilizar a informação no banco de dados do sistema de informação conforme prazos contratuais;

6.12.2 – Encerrar chamado e informar a restauração dos dados em banco de dados;

6.13 – Coordenador de Área – Tecnologia da Informação (IPACI) / Fiscal de Contrato

6.13.1 – Informar ao Usuário quanto ao Backup dos dados em sistema de Informação automatizado;

POLÍTICAS DE CONTROLE DE ACESSO LÓGICO

6.14 – Presidente Executivo

6.14.1 – Solicitar, através de ofício ou chamado Hespdesk, a criação/atualização de contas de acesso lógico à CTI e/ou Prestadores de Serviço de Sistema de Informação Automatizados, aos usuários do Instituto;

6.15 – Coordenadoria de Tecnologia da Informação – CTI (PMCI) e/ou Prestador de Serviço de Sistema de Informação Automatizado

6.15.1 – Criar usuário e senha provisória, sendo esses dados de cunho pessoal e intransferível, não podendo, de forma alguma, ser compartilhado com terceiros;

6.15.1.1 – As senhas deverão obedecer a uma combinação pré estabelecida, sendo estruturada da seguinte forma: mínimo de 08 (oito) caracteres, tendo necessariamente letras(s) maiúscula(s), letra(s) minúscula(s), dígito(s) numérico(s) ou caractere(s) especial;

6.15.1.2 – Por segurança, as senhas possuem um período de validade estabelecido pela Coordenadoria de Tecnologia da Informação. Ao final desse período, o usuário receberá uma solicitação para atualização da senha;

6.15.2 – Encaminhar via ofício ou chamado helpdesk, o login e senha do usuário criado/alterado, orientando-o de sua utilização e prestando o suporte necessário para o primeiro login;



6.16 – Presidente Executivo

6.16.1 – Encaminhar à Coordenador de Área – Tecnologia da Informação (IPACI) para verificar o atendimento às solicitações e suporte necessário para o primeiro login;

6.17 – Coordenador de Área – Tecnologia da Informação (IPACI) / Fiscal de Contrato

6.17.1 – Analisar o pedido realizado com a solicitação atendida e orientar aos usuários quanto ao suporte necessário para o primeiro login;

6.18 – Usuários

6.18.1 – Utilizar login e senha nos termos da Política de Segurança da Informação e Decreto Municipal nº 30.492/2021.

6.18.2 – Atualizar senhas sempre que solicitado pelo sistema ou que ameaças possam fragilizar a segurança desta.

CONTROLE DE ACESSO FÍSICO AO AMBIENTE TECNOLÓGICO DO IPACI

6.19 – Usuários Externos / Prestadores de Serviços

6.19.1 – Requerer acesso ao Ambiente Tecnológico do Instituto à Diretoria Administrativa;

6.20 – Diretoria Administrativa

6.20.1 – Analisar solicitação de acesso ao Ambiente Tecnológico do Instituto;

6.20.1.1 – Em caso de deferimento, solicitar que o Coordenador de Área – Tecnologia da Informação (IPACI) dê acesso aos Usuários Externos / Prestadores de Serviços e que acompanhe os trabalhos realizados por estes;

6.20.1.2 – Em caso de Indeferimento, fica proibido o acesso dos Usuários Externos / Prestadores de Serviços às dependências do Ambiente Tecnológico do Instituto;

6.21 – Coordenador de Área – Tecnologia da Informação (IPACI)

6.21.1 – Dá acesso aos Usuários Externos / Prestadores de Serviços e acompanhar os trabalhos realizados por estes;

6.21.2 – Dar feedback à Diretoria Administrativa, quanto aos trabalhos realizados pelo Usuários Externos / Prestadores de Serviços.

7. Considerações Finais:

7.1 – Para proteção da informação, previsto nos itens 3.1, alínea “h” e 3.8 da Política de Segurança da Informação (cópia de segurança), todos os dados de caráter imprescindível para o devido funcionamento regulamentar do IPACI deve ser obrigatoriamente armazenado no diretório de arquivos do Servidor de Arquivos, disponibilizado dentro do Servidor da Prefeitura Municipal de Cachoeiro de Itapemirim (PMCI) a fim de inclusão das informações na rotina de *backup*.

7.2 – Os serviços de cópias de segurança de contingência do IPACI é realizado pela Prefeitura Municipal de Cachoeiro de Itapemirim nos termos previstos no decreto nº 30.492/2021, sendo



a cargo do Coordenador de Área – Tecnologia da Informação (IPACI) realizar o contato primário com o serviço de Helpdesk disponibilizado pela PMCI para eventuais solicitações, entretanto é facultado a outros colaboradores do Instituto um contato via telefone conforme ocasional indisponibilidade do Setor de TI.

7.3 – É de responsabilidade do usuário manter uma cópia de segurança em mídia remota dos arquivos armazenados em seus computadores. Os arquivos salvos somente nas estações de trabalho não possuem garantia de backup. A Coordenadoria de Tecnologia da Informação não se responsabilizará pela perda desses arquivos;

7.4 – As informações omissas nesta IN será disciplinada pelo constante no Decreto Municipal nº 30.492/2021 e na Política de Segurança da Informação do Instituto;

7.5 – A Coordenação Executiva do Controle Interno verificará, por intermédio da Diretoria Administrativa, o exato cumprimento desta norma.

8. Siglas:

CTI – Coordenadoria de Tecnologia da Informação

IPACI– Instituto de Previdência de Cachoeiro de Itapemirim – ES

PMCI – Prefeitura Municipal de Cachoeiro de Itapemirim – ES

TI – Tecnologia da Informação



Anexo I – Fluxograma Cópia de Segurança de Servidor de
Arquivo e Sistemas de Informações Automatizados





