

Manual de Tecnologia da Informação

Regime Proprio de Previdência dos Servidores Públicos Municipais do Município de Colombo

Manual de Tecnologia da Informação	VERSÃO 1	APROVADO 07/2025
------------------------------------	-------------	---------------------

Sumário

1. Disposições Gerais.....	3
Apresentação.....	3
Objetivo.....	3
Aplicabilidade.....	3
2. Termos e Siglas Utilizados.....	3
3. Normas e Procedimentos Internos.....	4
4. Controles de Acesso	4
4.1 Acesso Lógico.....	4
4.1.1. Detalhamento do Processo.....	5
4.2 Acesso Físico.....	6
4.2.1 Detalhamento do Processo.....	7
5. Dos Backups	7
5.1 Detalhamento do Processo.....	8
6. Considerações Finais.....	9
7. Termo de Aprovação	10

1. DISPOSIÇÕES GERAIS

Apresentação

O presente Manual é de uso institucional da COLOMBO PREVIDÊNCIA - Previdência dos servidores Públicos Municipais de Colombo, e tem como principal objetivo aprimorar e padronizar processos de trabalho e instrumentos de controle. Visa padronizar os procedimentos realizados nos setores desta Autarquia, constituindo-se em um instrumento auxiliar no cumprimento de atribuições, servindo como fonte de orientação, contribuindo para aprimoramento do controle interno.

Contudo, este manual não esgota o assunto, muito pelo contrário, é o marco inicial para que seja aplicado no dia-a-dia, enriquecido pelas críticas e sugestões de melhorias de toda a equipe. Para atender aos seus objetivos, deverá ser permanentemente atualizado e aprimorado, de forma a acompanhar a evolução das atividades desenvolvidas, das técnicas de auditoria/inspeção e da administração pública municipal.

Objetivo

O objetivo deste material é dar entendimento quanto às informações necessárias nos procedimentos de Tecnologia da Informação estabelecendo procedimentos de contingência que determinem a existência de cópias de segurança dos sistemas informatizados e dos bancos de dados.

Nortear a definição de normas e procedimentos específicos de segurança da informação, bem como a implementação de controles e processos para seu atendimento.

Aplicabilidade

Todas as informações contidas neste Manual, deverão ser seguidas por todos os colaboradores da Autarquia, que tem a obrigação de manter-se atualizados em relação ao conteúdo deste material, buscando orientação do seu gestor ou área de tecnologia da informação caso haja dúvida em como agir em situação que pode ocasionar algum tipo de incidente.

2. Termos e Siglas utilizadas

2.1. Backup: Cópia de segurança de informações armazenada em meio magnético.

2.2. Chave de Acesso/Conta/Login: Código de acesso atribuído a cada Usuário. A cada Chave de Acesso é associada uma senha individual e intransferível, destinada a identificar o Usuário, permitindo-lhe o acesso aos recursos disponíveis.

2.3. Segurança da informação: Preservação da confidencialidade, integridade e disponibilidade da informação. Autenticidade, responsabilidade e confiabilidade também fazem parte da segurança da informação.

2.4. Servidores de Rede: Computadores com hardware e software para atender demandas no ambiente computacional específico.

2.5. TI: Tecnologia da informação.

3. DAS NORMAS E PROCEDIMENTOS INTERNOS:

Dentro de uma organização, a unidade, departamento ou setor de Tecnologia da Informação é responsável por todas as suas funções de informática.

A Colombo Previdência não tem um departamento de Tecnologia da Informação (TI) em seu quadro de pessoal, fazendo a terceirização de suporte, sistema e guarda de arquivos digitais.

Com relação ao suporte técnico e manutenção de hardware, bem como backup nuvem é realizado pelas empresa contratadas via processo licitatório. E os softwares são locados, por meio de licitação.

Possui locação dos diversos sistemas de software técnicos utilizados pelo RPPS, como de gestão, financeiro, concessão de benefícios, compensação previdenciária, site, entre outros.

A Colombo Previdência, possui Política de Segurança da Informação, a qual deve ser de conhecimento de todos os servidores; colaboradores; conselheiros; fornecedores ou qualquer outro interessado que por ventura necessite acessar dados e informações armazenadas no RPPS.

As empresas contratadas se submetem às questões estabelecidas em Política de Segurança da Informação que acompanham os contratos firmados com a Colombo Previdência.

Caso ocorra qualquer dúvida relacionada a segurança da Informação, deve buscar auxílio do gestor antes de qualquer acesso e/ou liberação de informação.

4. DOS CONTROLES DE ACESSO:

4.1. Acesso Lógico¹

Controle de Acesso Lógico é um conjunto de procedimentos, medidas e uma combinação de hardwares e softwares com o objetivo de proteger dados, programas e sistemas, alocados num Ciberespaço, contra tentativas de acesso não autorizadas feitas por pessoas ou outros programas de computador.

Tem as funções de identificação e autenticação de usuários; alocação, gerência e monitoramento de privilégios; limitação, monitoramento e desabilitação de acessos; e prevenção de acessos não autorizados.

¹ <https://gestaodesegurancaprivada.com.br/controle-de-acesso-logico-o-que-e-qual-objetivo-e-para-que-serve/>

Esta diretamente ligado a Segurança da Tecnologia da Informação, que tem um papel estratégico nas organizações, pois é área responsável pelos processos de proteção de toda a estrutura da tecnologia da informação de uma organização.

A Colombo Previdência não dispõe de instalação de CPD ou Data Center em sua sede. Os servidores (equipamentos de informática) da Colombo Previdência estão hospedados dentro da autarquia em sala devidamente fechada e dentro de um gabinete com chave.

Embora não exista área de CPD ou Data Center na sede do Instituto, a sede possui sistema de câmera, alarme e sensores de presença com monitoramento por empresa contratada, sendo que somente os funcionários autorizados pelo setor administrativo possuem chave de acesso e controle remoto. A recepção possui guichê e somente funcionários e pessoas autorizadas podem acessar o lado interno da Colombo Previdência.

Todos os servidores ao saírem de suas respectivas salas devem trancar as portas de acesso externo.

Para garantir a segurança da informação, as empresas softwares, contratadas pela Colombo Previdência, apenas devem fornecer acesso às bases de dados lógicas do RPPS a servidores com autorização expressa do Gestor (a).

O acesso a cada um dos sistemas ocorre mediante login e senha exclusivos de cada usuário.

Para acesso aos sistemas contratados o Gestor da Colombo Previdência deverá notificar a empresa contratada (via e-mail, whatsapp ou telefone) por meio do suporte técnico para a criação de usuário e senha, devendo ser informado o nível de acesso a ser concedido, cargo, nome completo e CPF.

Para acesso nos computadores disponíveis a casa servidor/usuário terá acesso mediante senha pessoal e intransferível.

Cada servidor é responsável por salvar os arquivos editados, dentro das pastas dos respectivos setores.

4.1.1.Detalhamento do Processo

- a) Usuário que deseja ter acesso aos arquivos lógicos da Autarquia, deve solicitar aos dirigentes da instituição que o acesso seja liberado.
- b) Diretoria faz a análise do pedido concedendo ou não o acesso, e quando ocorrer a permissão deve esclarecer qual o período e pastas e sistemas que o usuário poderá acessar.
- c) Se não autorizado, arquiva-se a solicitação.
- d) Autorizado o acesso solicitado, é aberto chamado para a equipe de TI e/ou empresa provedora do sistema, contratada pela Autarquia, via e-mail/ whatsapp (suporte da empresa).
- e) A empresa contratada, faz a liberação do acesso e envia a autorização como resposta do chamado;
- f) O responsável pela concessão, envia por e-mail as credenciais de acesso para o usuário, quando for o caso.
- g) Cada funcionário deve possuir um ID/ "nome de usuário" e uma senha para acesso a rede. A partir destes, terá acesso as pastas de arquivos servidor, de acordo com a necessidade da função exercida.
- h) Assim que receber as credenciais, o usuário deve alterar sua senha para alguma de uso pessoal e intransferível.
- i) Periodicamente, a equipe de TI responsável pela atividade faz uma varredura em todos os acessos ativos para o usuário e bloqueia os acessos inativos ou não mais necessários, na base de dados.

- j) Todo e qualquer acesso remoto aos sistemas e servidores, se dará através do uso de um único nome de usuário e senha.
- k) Contas para prestadores de serviço, utilizadas para suporte e manutenção remota, serão habilitadas apenas durante o tempo necessário. Estes procedimentos serão acompanhados por funcionários da Autarquia ou da equipe de Tecnologia da Informação.
- l) Funcionários demitidos serão imediatamente removidos do Sistema, mediante solicitação do Dirigente à empresa contratada.
- m) Usuários que possuam acesso a informações críticas deverão estar cientes dos procedimentos relativos às senhas e seus respectivos regulamentos.
- n) Uma conta de usuário será automaticamente bloqueada após várias tentativas falhas de “login” no Sistema, conforme as regras e disposições de cada provedor . O desbloqueio deve ser habilitado pelo administrador responsável.
- o) O computador possuirá um “time-out” (tempo limite) de cinco minutos, ou seja, usuários inativos por mais de cinco minutos deverão realizar um novo “login” no sistema;

4.2 Acesso Físico²

Controle de acesso físico é a utilização de medidas de segurança física (passivas e ativas), e de protocolos de gerenciamento, projetados para impedir o acesso não autorizado a áreas, pessoal, equipamentos, documentos, e salvaguardá-los contra espionagem, sabotagem, danos, furto e roubo.

Refere-se às medidas de segurança física adotadas explorando se os meios físicos e tecnológicos disponíveis, utilizando-os como barreira de proteção ao acesso a um ambiente físico controlado e a ativos críticos.

É utilizado para gerenciar e controlar o fluxo de pessoas e bens físicos da organização.

O objetivo do controle de acesso físico não é proibir ou dificultar o acesso, mas controlá-lo. Ou seja, ele visa saber quem tem acesso concedido, quando o acesso é concedido, para onde e por que o acesso é concedido.

Ele visa proteger as pessoas, os bens e o conhecimento contra acessos não autorizados.

Um bom sistema de controle de acesso físico deve ser capaz de assegurar a entrada fácil e simplificada, das pessoas devidamente autorizadas, e detectar e/ou impedir o acesso de pessoas não autorizadas.

Ao final do expediente todos os servidores devem armazenar qualquer documento ou processo físico dentro de armários com chave, a fim de evitar que documentos fiquem expostos em local visível.

O arquivo físico da Colombo Previdência encontra-se acondicionado em sala separada da sede da Autarquia com câmera, alarme e sensores de presença com monitoramento por empresa contratada, sendo que somente os funcionários autorizados pelo setor administrativo possuem chave de acesso e controle remoto.

4.2.1 Detalhamento do Processo

- a) O interessado em acessar os dispositivos físicos da entidade, deve antes de qualquer ação, pedir autorização à Diretoria.
- b) Diretoria avalia o caso, e autoriza ou não o acesso aos dados.
- c) Se não autorizado, arquiva-se a solicitação.

² Texto retirado de : <https://gestaodesegurancaprivada.com.br/controle-de-acesso-fisico/>

- d) Se autorizado, faz o registro de acesso para controle .
- e) Visitantes, ou seja, pessoas que não fazem parte do quadro próprio de funcionários, precisam de autorização e acompanhamento para adentrar às áreas de acesso;
- f) Os processos físicos antes de serem devidamente arquivados, são catalogados por servidor responsável que colocará os dados e número da gaveta que será arquivado em planilha própria.
- g) Os processos de licitação físicos são arquivados em arquivos de acesso com chefe e somente manipulados por servidor devidamente autorizado;
- h) Os demais documentos físicos, como ofícios e memorando são arquivados em pasta própria e arquivados em armário com chave durante o ano em exercício, e posteriormente são arquivados na sala de arquivo em prateleira própria.

5. DOS BACKUPS:

Na Administração Pública é recente a preocupação com a gestão dos documentos arquivísticos. Mas, com o avanço do uso dos meios digitais nas repartições públicas, o papel está perdendo espaço.

Sobretudo pela praticidade e economicidade de espaço físico, já que um arquivo físico demanda um investimento com armazenamento, acondicionamento e condições ambientais adequadas.

Mas, é cedido que a guarda de documentos deve ser prioridade em qualquer organização tanto pública como privada, pois é a forma que elas possuem para comprovar o cumprimento de uma obrigação e prestação de contas.

Assim, independentemente de o arquivo ser em papel ou digital, os documentos precisam ser guardados e, principalmente, conservados. No RPPS não é diferente.

Devido ao crescimento da produção dos documentos digitais há de se ressaltar a preocupação com o acesso dos documentos digitais ao longo do tempo, a fim de garantir sua autenticidade e legalidade.

Com o surgimento da Lei nº 12.527, de 2011, a Lei de Acesso à Informação, houve a regulamentação do direito constitucional de acesso às informações públicas e o dever de ofício da Administração Pública de promover a transparência de seus atos para a sociedade.

Assim, a importância de organizar, divulgar e de preservar as informações arquivísticas ganhou uma grande relevância e a implementação de um sistema informatizado passou a ser fundamental para gerir corretamente a informação arquivística. Dentro da Autarquia ainda há alguns documentos que são arquivados fisicamente, principalmente porque ainda não há a possibilidade de guarda exclusivamente digital, que deveria ser autorizada por Lei, para alguns tipos de documentos.

Com o conhecimento da importância da guarda e preservação dos dados do RPPS, serão realizadas cópias de segurança dos sistemas informatizados e dos bancos de dados do RPPS, das seguintes formas:

- As cópias de segurança dos bancos de dados dos sistemas informatizados são realizadas de acordo com as disposições contratuais com cada fornecedor.
- Os backups dos arquivos do servidor acontecerão diariamente nos termos definidos na Política de Segurança da Informação – PSI, realizados pela empresa de Tecnologia da Informação contratada.

5.1. Detalhamento do processo

a) Da recuperação de dados da rede do servidor local

Em caso de danos causados no servidor local, armazenado na sede da Autarquia, a Diretoria deverá abrir chamado à empresa contratada para recuperação de backup em nuvem.

Deve a Diretoria verificar, com auxílio da empresa de Tecnologia da Informação, quais os procedimentos de recuperação do equipamento do servidor para correto funcionamento;

Será feita análise de possíveis soluções temporárias para que não sejam interrompidos os serviços prestados pelo RPPS durante o período de recuperação dos dados;

Com soluções temporárias definidas, deverão ser comunicados todos os colaboradores dos meios e formas de trabalho, neste período.

Após a solução e recuperação dos dados de rede, serão reestabelecidos os padrões normais de trabalho, devendo ser comunicados os colaboradores, caso tenha ocorrido alguma alteração.

b) Da recuperação dos dados de sistemas operacionais

Em caso de danos/ perdas de informações dos sistemas operacionais, o colaborador que perceber tal situação deverá imediatamente comunicar a Diretoria e Fiscal do Contrato;

Deverá abrir chamado ao provedor do sistema relatando o ocorrido e solicitando a imediata correção, nos termos contratuais.

Deverão ser analisadas possíveis soluções até que se reestabeleçam as condições normais de trabalho no sistema, bem como banco de dados.

Após a solução e recuperação dos dados do sistema, serão reestabelecidos os padrões normais de trabalho, devendo ser comunicados os colaboradores, caso tenha ocorrido alguma alteração.

6. CONSIDERAÇÕES FINAIS

Destacamos que o presente manual é passível de alterações e adequações conforme as necessidades da administração. Deverão ser utilizados como “roteiros” de trabalho e não exclusivamente como único meio de pesquisa, devendo todos os servidores envolvidos sempre observar demais legislações e regras a serem aplicadas ao caso concreto, especialmente a Política de Segurança de Informação da Colombo Previdência.

TERMO DE APROVAÇÃO

O presente Manual de Tecnologia da Informação foi revisado pela Equipe Técnica e aprovado pela Diretoria Executiva da Colombo Previdência, estando todos os presentes cientes de seu conteúdo.

Dê-se publicidade e conhecimento aos servidores da Autarquia.

Colombo, 01 de Julho de 2024.

Wilton Luiz Carrão
Diretor Superintendente

Giovani Corletto
Diretor Financeiro

Aleksandra do Carmo Ullmann
Diretora de Gestão Previdenciária