Estado do Rio de Janeiro
Município de Macaé
Instituto de Previdência Social
Comissão Pró-Gestão

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

DIRETRIZES E NORMAS INSTITUCIONAIS

Versão 1.0

SUMÁRIO

1 - APRESENTAÇÃO

A Política de Segurança da Informação (PSI) é o documento que orienta e estabelece as diretrizes corporativas do Instituto de Previdência Social do Município de Macaé para a proteção dos ativos de informação e a prevenção de responsabilidade legal para todos os usuários. Deve, portanto, ser cumprida e aplicada em todas as áreas da instituição. A presente PSI está baseada nas recomendações propostas pela norma ABNT NBR ISO/IEC 27002:2013, reconhecida mundialmente como um código de prática para a gestão da segurança da informação, bem como está de acordo com as leis vigentes em nosso país, incluindo a Lei Geral de Proteção de Dados Pessoais (LGPD – Lei 13.709, 14 de agosto de 2018).

2 - OBJETIVO

Garantir que os recursos computacionais e serviços de Tecnologia da Informação (TI) serão utilizados de maneira adequada. O usuário deve conhecer as regras para utilização da informação de maneira segura, evitando exposição que possa prejudicar o Macaeprev, colaboradores e terceiros. A Política deve implementar controles para preservar os interesses do instituto contra danos que possam acontecer devido falha na segurança. Ela deve descrever as normas de utilização e possíveis atividades que possam ser consideradas como violação ao uso dos serviços, portanto, considerados proibidos. Segundo a norma ABNT ISO/IEC27002:2013, deve preservar as informações do Macaeprev, quanto à:

• **Integridade**: garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais.

• **Confidencialidade**: garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.

• **Disponibilidade**: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

As normas descritas no decorrer devem sofrer alterações sempre que necessário, sendo que estas devem ser registradas pela equipe de Tecnologia da Informação (TI), aprovadas

pelo Setor de Segurança da Informação e divulgadas pelo Setor de TI, dentro da estrutura de processo organizacional do Macaeprev, considerando-se o tempo hábil para que eventuais providências sejam tomadas. Tais normas devem ser observadas por todos os usuários. Em caso de dúvida o usuário deverá procurar o Setor de Tecnologia de Informação, para maiores esclarecimentos. Caso os procedimentos ou normas aqui estabelecidos sejam violados por usuários, o Setor de Tecnologia da Informação informará aos órgãos competentes de forma que sejam tomadas as medidas cabíveis. Esta política aplica-se a todos os usuários dos recursos computacionais e serviços de TI.

3 - JUSTIFICATIVA

A segurança da informação é crucial nos dias atuais, principalmente, se levar em consideração os números expressivos de incidentes de segurança da informação reportados ao Centro de Estudos e Tratamento de Incidentes de Segurança no Brasil (CERT.br). Segundo o CERT.br (2020), foram notificados 665.079 incidentes de segurança no país no ano de 2020. Este é um número expressivo de ataques cibernéticos, e deve-se destacar, que muitas das instituições atacadas são órgãos governamentais, como prefeituras, estados, entre outras.

Segundo o cálculo atuarial 2021 (ano base 2020), o instituto consta com 13.577 servidores ativos em sua base de dados, 1.315 aposentados e 389 pensionistas. O volume dos ativos garantidores do plano de benefícios retratado no cálculo atuarial recente é muito expressivo, e segundo informações no site SPREV, o município de Macaé configura entre os vinte primeiros RPPS com maior quantidade de ativos financeiros. O que o torna um órgão governamental com bastante visibilidade no cenário nacional. Com isso, é importante estabelecer normas e práticas que ajudem a prevenir a saúde institucional e financeira do Macaeprev.

Outro fator relevante para consolidação da implantação da PSI, é que ela se constitui um item importante e obrigatório nos quesitos especificados pelo Governo Federal no Manual de Programa Pró-gestão versão 3.2. O Pró-gestão é o Programa de Certificação Institucional e Modernização da Gestão dos Regimes Próprios de Previdência Social da União, dos Estados, do Distrito Federal e dos Municípios, implantado pela Secretaria da Previdência.

4 - DEFINIÇÕES

CERT.br – Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil.

LGPD – Lei Geral de Proteção de Dados Pessoal.

Macaeprev – Instituto de Previdência Social do Município de Macaé.

TI - Tecnologia da Informação, pode ser definida como o conjunto de todas as atividades e soluções providas por recursos de computação que visam a produção, o armazenamento, a transmissão, o acesso, a segurança e o uso das informações.

Usuários – Toda e qualquer pessoa, física ou jurídica, que utilize os recursos computacionais e serviços de TI do Macaeprev. Também considerados servidores/colaboradores.

Recursos computacionais - são ativos de tecnologia da informação, administrados, mantidos ou operados pela Macaeprev, tais como:

- Computadores e terminais de qualquer espécie, incluídos seus acessórios;
- Periféricos e afins;
- Redes de computadores e de transmissão de dados e seus acessórios;
- Dispositivos de segurança e sistemas de energia elétrica;
- Discos, mídias, fitas e meios de armazenamentos;
- Bancos de dados ou informações ou documentos residentes em disco, mídia, fita ou outros meios de armazenamentos;
- Ambientes informatizados;
- Serviços e informações disponibilizados via a arquitetura de informática da instituição;
- Softwares e hardwares adquiridos ou desenvolvidos.
- Serviços de TI - de acordo com o *Information Technology Infrastructure Library* (ITIL) é um serviço provido para um ou mais clientes por um provedor de serviços, que suporta os processos de negócios deste (s) cliente (s), é feito de uma combinação de pessoas, processos e tecnologia e deve ser definido por acordos de nível de serviço".

5 - ATRIBUIÇÃO DE RESPONSABILIDADES PARA SEGURANÇA DA INFORMAÇÃO

O cumprimento da PSI é obrigatório a todos os usuários (servidores estatutários, comissionados, prestadores de serviço, estagiários) do Macaeprev. É dever de todos também informar ao setor de TI qualquer incidente de segurança da informação observado, para que sejam tomadas medidas protetivas à segurança da informação do instituto. É responsabilidade da presidência e diretorias, órgãos colegiados e coordenações fazer cumprir e propiciar a todos os servidores o acesso a PSI.

6 - CLASSIFICAÇÃO DA INFORMAÇÃO

Cabe aos diretores/coordenadores de cada setor estabelecer os critérios quanto ao nível de confidencialidade da informação produzida por seu respectivo setor, seguindo as seguintes classificações:

- **Pública**: é toda informação dedicada ao público em geral, tanto interno, quanto externo, sendo informativa, educacional, promocional.
- **Corporativa**: é toda informação que deve ser acessada apenas pelos usuários do Macaeprev, de acordo com o respectivo setor ao qual estes pertencem.
- **Confidencial**: constitui-se numa informação crítica para o instituto ou seus beneficiários e patrocinadores. A divulgação desta pode vir a causar danos e impactos ao instituto ou aos seus patrocinadores/segurados.

7 - POLÍTICA DE SEGURANÇA DA ESTRUTURA DE TECNOLOGIA DA INFORMAÇÃO

Abrange itens relacionados à utilização desta estrutura, como política de utilização da rede, utilização e administração de contas, senhas, correio eletrônico, acesso à Internet, uso das estações de trabalho, utilização de impressoras, etc.

7.1 - POLÍTICA DE UTILIZAÇÃO DA REDE

7.1.1 - Identificação

Os dispositivos de identificação e senhas protegem a identidade do colaborador usuário, evitando e prevenindo que uma pessoa se faça passar por outra perante o Instituto de Previdência Social de Macaé ou terceiros. O uso dos dispositivos e/ou senhas de identificação de outra pessoa constitui crime tipificado no Código Penal Brasileiro (art. 307 – falsa identidade). Tal norma visa estabelecer critérios de responsabilidade sobre o uso dos dispositivos de identificação e deverá ser aplicada a todos os colaboradores. Todos os dispositivos de identificação utilizados no Macaeprev, como o número de registro do colaborador, as identificações de acesso aos sistemas, os certificados e assinaturas digitais e os dados biométricos têm de estar associados a uma pessoa física e atrelados inequivocamente aos seus documentos oficiais reconhecidos pela legislação brasileira. O usuário, vinculado a tais dispositivos identificadores, será responsável pelo seu uso correto perante a instituição e a legislação (cível e criminal). Todo e qualquer dispositivo de identificação pessoal, portanto, não poderá ser compartilhado com outras pessoas em nenhuma hipótese. É proibido o compartilhamento de login para funções de administração de sistemas. Devem ser distintamente identificados os visitantes, estagiários, empregados temporários, empregados regulares e prestadores de serviços, sejam eles pessoas físicas e/ou jurídicas. É de responsabilidade de cada usuário a memorização de sua própria senha, bem como a proteção e a guarda dos dispositivos de identificação que lhe forem designados. Todos os acessos devem ser imediatamente bloqueados quando se tornarem desnecessários. Portanto, assim que algum usuário for afastado, o Departamento/Divisão onde o mesmo trabalhava deverá imediatamente comunicar tal fato à Coordenadoria de Tecnologia da Informação, a fim de que essa providência seja tomada. O

mesmo procedimento deve ser feito pelo usuário afastado, uma vez que o usuário e senha são de total responsabilidade dele. A mesma conduta se aplica aos usuários cujo contrato ou prestação de serviços tenha se encerrado, bem como aos usuários de testes e outras situações similares. Caso o colaborador esqueça sua senha, ele deverá requisitar formalmente a troca ou comparecer pessoalmente à área técnica responsável para cadastrar uma nova.

7.1.2 - Computadores e recursos tecnológicos

Os equipamentos disponibilizados aos usuários são de propriedade do Macaeprev, cabendo a cada um utilizá-los e manuseá-los corretamente para as atividades de interesse da instituição, bem como cumprir as recomendações constantes nos procedimentos operacionais fornecidos pelas diretorias responsáveis. É proibido todo procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação, sem o conhecimento prévio e o acompanhamento de um técnico do Setor de Tecnologia da Informação, ou de quem este determinar. As Diretorias que necessitarem fazer testes deverão solicitá-los previamente ao Setor de Tecnologia da Informação, ficando responsáveis jurídica e tecnicamente pelas ações realizadas. Todas as atualizações e correções de segurança do sistema operacional ou aplicativos somente poderão ser feitas após a devida validação no respectivo ambiente de homologação, e depois de sua disponibilização pelo fabricante ou fornecedor. Os sistemas e computadores devem ter versões do software antivírus instaladas, ativadas e atualizadas permanentemente. O usuário, em caso de suspeita de vírus ou problemas na funcionalidade, deverá acionar o departamento técnico responsável mediante registro de chamado no atendimento. A transferência e/ou a divulgação de qualquer software, programa ou instruções de computador para terceiros, por qualquer meio de transporte (físico ou lógico), somente poderá ser realizada com a devida identificação do solicitante, se verificada positivamente e estiver de acordo com a classificação de tal informação e com a real necessidade do destinatário. Arquivos pessoais e/ou não pertinentes ao negócio do Macaeprev (fotos, músicas, vídeos, etc..), não deverão ser copiados/movidos para os drives de rede, pois podem sobrecarregar o armazenamento nos servidores. Caso identificada a existência desses arquivos, eles poderão ser excluídos definitivamente com ou sem comunicação prévia ao usuário. Documentos imprescindíveis para as atividades dos colaboradores da instituição deverão ser salvos em drives

de rede. Tais arquivos, se gravados apenas localmente nos computadores (por exemplo, no drive C:), não terão garantia de backup e poderão ser perdidos caso ocorra uma falha no computador, sendo, portanto, de responsabilidade do próprio usuário. É expressamente proibido o consumo de alimentos, bebidas ou fumo na mesa de trabalho e próximo aos equipamentos. Deverão ser protegidos por senha (bloqueados), todos os terminais de computador e impressoras quando não estiverem sendo utilizados. Todos os recursos tecnológicos adquiridos pelo Macaeprev devem ter imediatamente suas senhas padrões (*default*) alteradas. Os equipamentos deverão manter preservados, de modo seguro, os registros de eventos, constando identificação dos colaboradores, datas e horários de acesso. Algumas situações em que é proibido o uso de computadores e recursos tecnológicos do instituto:

• Tentar ou obter acesso não autorizado a outro computador, servidor ou rede.

• Burlar quaisquer sistemas de segurança.

• Acessar informações confidenciais sem explícita autorização do proprietário.

• Vigiar secretamente outrem por dispositivos eletrônicos ou softwares, como, por exemplo, analisadores de pacotes (*sniffers*).

• Interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado.

• Usar qualquer tipo de recurso tecnológico para cometer ou ser cúmplice de atos de violação, assédio sexual, perturbação, manipulação ou supressão de direitos autorais ou propriedades intelectuais sem a devida autorização legal do titular;

• Hospedar ou acessar pornografia, material racista ou qualquer outro que viole a legislação em vigor no país, a moral, os bons costumes e a ordem pública.

• Utilizar software pirata, atividade considerada delituosa de acordo com a legislação nacional.

7.1.3 - Solicitação de acesso

O usuário deverá fazer uma solicitação da criação da conta, através do formulário eletrônico, disponível na Intranet pelo endereço http://macae.rj.gov.br/macaeprev. Neste formulário, deverão ser informados os dados do usuário, bem como os acessos que serão necessários para que este usuário desempenhe suas funções na área (diretórios da rede Macaeprev, acesso aos sistemas do instituto. Após o preenchimento do formulário, o mesmo deverá ser impresso e autorizado pelo secretário da pasta, e encaminhado ao setor de Tecnologia da Informação. A equipe de TI retornará carta senha para departamento, via protocolo ou e-mail informado. Informações sobre a conta criada, assim como orientações como alteração imediata de senha serão fornecidas ao receber a carta senha e as normas.

7.2 - Política de utilização de e-mail

O objetivo desta norma é informar aos servidores/colaboradores do Macaeprev quais são as atividades permitidas e proibidas quanto ao uso do e-mail corporativo. O uso do e-mail do Macaprev é para fins corporativos e relacionados às atividades do usuário dentro da instituição. A utilização desse serviço para fins pessoais é permitida desde que feita com bom senso, não prejudique o Macaeprev e também não cause impacto no tráfego da rede.

O e-mail deve ser utilizado de forma consciente, evitando qualquer tipo de perturbação a outras pessoas, seja através da linguagem utilizada, frequência ou tamanho das mensagens; O envio deve ser efetuado somente para pessoas que desejam recebê-los. Se for solicitada a interrupção, esta deve ser acatada e não deverá mais acontecer. É proibido o envio de grande quantidade de mensagens de e-mail (*spam*) que, de acordo com a capacidade técnica da rede, seja prejudicial ou gere reclamações de outros usuários. Isso inclui qualquer tipo de mala direta, como por exemplo, publicidade, comercial ou não, anúncios e informativos, ou propaganda política. Situações em que é proibido aos colaboradores o uso do e-mail corporativo:

- Enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas a uso legítimo da instituição;

- Enviar mensagem por correio eletrônico pelo endereço de seu departamento ou usando o nome de usuário de outra pessoa ou endereço de correio eletrônico que não esteja autorizado a utilizar;
- Enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou o Macaeprev vulnerável a ações civis ou criminais;
- Divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário desse ativo de informação;
- Falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ ou destinatários, com o objetivo de evitar as punições previstas.
- Enviar e-mails de cunho político e ou partidário.

É obrigatória a utilização de assinatura nos e-mails, seguindo padrão estabelecido pelo Macaeprev.

7.3 - Política de Acesso a internet

Estas regras visam basicamente o desenvolvimento de um comportamento ético e profissional do uso da internet no Macaeprev. Embora a conexão direta e permanente da rede corporativa da instituição com a internet ofereça um grande potencial de benefícios, ela abre a porta para riscos significativos para os ativos de informação. Qualquer informação que é acessada, transmitida, recebida ou produzida na internet está sujeita a divulgação e auditoria. Portanto, o Setor de Tecnologia da Informação, em total conformidade legal, reserva-se o direito de monitorar e registrar todos os acessos a ela. Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet são de propriedade do instituto, que pode analisar e, se necessário, bloquear qualquer arquivo, site, correio eletrônico, domínio ou aplicação armazenados na rede/internet, estejam eles em disco local, na estação ou em áreas privadas da rede, visando assegurar o cumprimento de sua Política de Segurança da Informação. O Setor de Tecnologia da Informação, ao monitorar a rede interna, pretende garantir a integridade dos dados e programas. Toda tentativa de alteração dos parâmetros de segurança, por qualquer colaborador, sem o devido credenciamento e a autorização para tal, será julgada inadequada e

os riscos relacionados serão informados ao colaborador e ao respectivo gestor. O uso de qualquer recurso para atividades ilícitas poderá acarretar as ações administrativas e as penalidades decorrentes de processos civil e criminal, sendo que nesses casos a instituição cooperará ativamente com as autoridades competentes. A internet disponibilizada pela instituição aos seus colaboradores, independentemente de sua relação contratual, pode ser utilizada para fins pessoais, desde que não prejudique o andamento dos trabalhos na instituição. É proibida a divulgação e/ou o compartilhamento indevido de informações da área administrativa em listas de discussão, sites ou comunidades de relacionamento, salas de bate-papo ou chat, comunicadores instantâneos ou qualquer outra tecnologia correlata que venha surgir na internet. O uso, a instalação, a cópia ou a distribuição não autorizada de softwares que tenham direitos autorais, marca registrada ou patente na internet são expressamente proibidos. Os usuários não poderão em hipótese alguma utilizar os recursos do Macaeprev para fazer o download ou distribuição de software ou dados pirateados, atividade considerada delituosa de acordo com a legislação nacional.

7.4 - Backup

Todos os *backups* devem ser automatizados por sistemas de agendamento automatizado para que sejam preferencialmente executados fora do horário comercial, nas chamadas "janelas de *backup*" – períodos em que não há nenhum ou pouco acesso de usuários ou processos automatizados aos sistemas de informática. Os colaboradores responsáveis pela gestão dos sistemas de *backup* deverão realizar pesquisas frequentes para identificar atualizações de correção, novas versões do produto, ciclo de vida (quando o software não terá mais garantia do fabricante), sugestões de melhorias, entre outros. As mídias de backup (como DAT, DLT, LTO, DVD, CD e outros) devem ser acondicionadas em local seco, climatizado, seguro (de preferência em cofres corta-fogo segundo as normas da ABNT) e distantes o máximo possível do *Datacenter*. As fitas de *backup* devem ser devidamente identificadas, inclusive quando for necessário efetuar alterações de nome, e de preferência com etiquetas não manuscritas, dando uma conotação mais organizada e profissional. O tempo de vida e uso das mídias de *backup* deve ser monitorado e controlado pelos responsáveis, com o objetivo de excluir mídias que possam apresentar riscos de gravação ou de restauração decorrentes do uso

prolongado, além do prazo recomendado pelo fabricante. Testes de restauração (*restore*) de *backup* devem ser executados por seus responsáveis, nos termos dos procedimentos específicos, aproximadamente a cada 90 ou 120 dias, de acordo com a criticidade do backup. Para formalizar o controle de execução de *backups* e *restores*, deverá ser encaminhada uma solicitação através de sistema homologado para a equipe de Segurança da Informação. A notificação da necessidade de backup ficará a cargo do colaborador/usuário solicitar. Todos os usuários devem salvar seus arquivos nas pastas da rede corporativa. Não haverá garantia de backups de arquivos salvados fora das unidades de pastas organizacionais. O *backup* realizado no instituto segue os seguintes procedimentos: é realizado backup full no sábado; *backup* incremental todos os outros dias às 18h00min; cópia de sombra de servidor de dados diariamente às 07h00min da manhã e 12h00min da tarde.

7.5 – Datacenter

O acesso ao *Datacenter* somente deverá ser feito por sistema forte de autenticação. Por exemplo: tranca, cadeado, fechadura eletrônica, biometria, cartão magnético entre outros. O acesso de visitantes ou terceiros somente poderá ser realizado com acompanhamento de um colaborador autorizado. O Datacenter deverá ser mantido limpo e organizado. Qualquer procedimento que gere lixo ou sujeira nesse ambiente somente poderá ser realizado com a colaboração do Departamento de Serviços Gerais. Não é permitida a entrada de nenhum tipo de alimento, bebida, produto fumígeno ou inflamável. A temperatura, umidade e ventilação das instalações que abrigam equipamentos de informática e de comunicações, devem estar de acordo com os padrões técnicos especificados pelos fabricantes dos equipamentos. No caso de perda de chaves de departamentos ou laboratórios a coordenação responsável deve ser informada imediatamente para que possa providenciar a troca das fechaduras.

8 - CONTINGÊNCIA DOS SERVIÇOS DE TI

Um plano de contingência consiste em uma análise de riscos que uma organização está sujeita, considerando seus recursos computacionais disponíveis para definir melhores práticas a serem adotadas em falhas técnicas, incidentes de segurança da informação, desastres

naturais, entre outros sinistros. Um plano de contingência é essencial para toda empresa que dependa de TI para seu funcionamento operacional. Principalmente, os sistemas informatizados automatizados, que são a base dos processos de negócios da organização. Portanto, é necessário que seu funcionamento sofra nenhuma ou menor número possíveis de interrupções. Para garantir a alta disponibilidade de TI, uma prática recomendável é implementar redundância nos recursos computacionais, que significa a duplicação de componentes/serviços críticos, reduzindo o risco de falhas iminentes. E para implementar redundância em nível macro, o instituto trabalha com virtualização. Existem dois servidores de virtualização, que com a interrupção de funcionamento de um, o outro servidor assume a operacionalização. Há também redundância elétrica, pois nos servidores há duas fontes de alimentação de energia. Para manutenção de funcionamento dos serviços web, há redundância de link de internet, para caso haja falha em um link, o outro assuma o serviço na rede interna do instituto. Estes são procedimentos básicos e padrões obrigatórios para garantia de alta disponibilidade institucional no Macaeprev.

9 - TERMO DE COMPROMISSO

O termo de compromisso é utilizado para que usuários se comprometam formalmente em seguir a política de segurança, tomando ciência das punições impostas ao seu não cumprimento. No termo de compromisso são reforçados os principais pontos da política de segurança e todos os servidores e demais colaboradores deverão tomar ciência. Sua renovação deve ser feita sempre que necessário. Disponível em: http://macae.rj.gov.br/macaeprev/.

10 - VIOLAÇÃO DA POLÍTICA, ADVERTÊNCIA E PUNIÇÕES

Ao se detectar uma violação da política, a primeira ação a fazer é determinar a sua razão, ou seja, verificar se a violação ocorreu por negligência, acidente, erro ou por desconhecimento da política vigente. E como procedimento da PSI, O setor de Tecnologia da Informação procederá ao bloqueio do acesso ou ao cancelamento do usuário, caso seja detectado uso indevido com o intuito de prejudicar o andamento do trabalho ou pôr em risco a

imagem da instituição. É recomendado o treinamento dos usuários em segurança da informação, por meio de cartilhas, com o intuito de divulgar e conscientizar os servidores e demais colaboradores sobre a política de segurança a ser seguida por todos. O programa de treinamento em segurança deve fazer parte do programa de integração de novos usuários. Os treinamentos de reciclagem devem ser previstos quando necessários. Caso seja necessário advertir o usuário pelo não cumprimento das normas estabelecidas neste documento, devem ser informados o superior imediato e o departamento de Recursos Humanos para interagir e se manterem informados da situação. Conforme previsto no Regime Jurídico dos Servidores Públicos Municipais, Lei Complementar 011/1998, o servidor/colaborador poderá ser aplicada a penalidade no caso da irregularidade comprovada. De acordo com a infração cometida, as seguintes punições serão: comunicação de descumprimento, advertência ou suspensão e demissão por justa causa.

Comunicação de descumprimento: Será encaminhado ao servidor, por e-mail, comunicado informando o descumprimento da norma, com a indicação precisa da violação praticada. Cópia desse comunicado permanecerá arquivada junto ao Departamento de Recursos Humanos na respectiva pasta do servidor/colaborador.

Advertência ou suspensão: A pena de advertência ou suspensão será aplicada, por escrito, somente nos casos de natureza grave ou na hipótese de reincidência na prática de infrações de menor gravidade.

Demissão por justa causa: Nas hipóteses previstas no estatuto do servidor municipal. Fica desde já estabelecido que não há progressividade como requisito para a configuração da dispensa por justa causa, podendo a Diretoria, no uso do poder diretivo e disciplinar que lhe é atribuído, aplicar a pena que entender devida quando tipificada a falta grave.

Responsáveis:

Cláudio de Freitas Duarte
Presidente - MACAEPREV
Matr. 3333-2 - CMM

Júlio César V. Carlos
Diretor Previdenciário
MACAEPREV - Matr. 42.398-PMM

Data: 14/09/2021

José Eduardo da Silva Guimarães
Diretor Financeiro
PMM Matr 17 339

PMM - 17336