(13) 3343-9050
@guarujaprevidencia
@guarujaprevidencia
guarujaprevidencia.sp.gov.br
Av. Adhemar de Barros, 230 - Bairro Santo Antônio
Guarujá/SP - CEP 11430 - 000

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO - TECNOLOGIA DA INFORMAÇÃO - TI

1. INFORMAÇÃO

Entenda-se “informação” como qualquer conteúdo que possa gerar entendimento sobre determinado assunto para algum indivíduo. A Informação pode assumir diversas formas: O conhecimento de uma pessoa, o armazenamento eletrônico, um impresso, uma anotação e a transmissão eletromagnética, visual ou auditiva. Segurança da Informação são esforços contínuos para a proteção dos ativos de informação, auxiliando a GuarujáPrev a cumprir sua missão.

2. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

2.1 Objetivos da Política de Segurança da Informação

Garantir a disponibilidade, integridade, confidencialidade, legalidade e autenticidade da informação necessária para a realização dos objetivos da GuarujáPrev.

- **Disponibilidade:** garantir que as informações estejam disponíveis a todas as pessoas autorizadas a tratá-las.
- **Integridade:** garantir que as informações sejam mantidas íntegras, sem modificações indevidas – acidentais ou propositais;
- **Confidencialidade:** garantir que as informações tratadas sejam de conhecimento exclusivo de pessoas especificamente autorizadas;
- **Legalidade:** o uso da informação deve estar de acordo com as leis aplicáveis, regulamentos, licenças e contratos.
- **Autenticidade:** validar a autorização do usuário para acessar sistemas, informações etc. Isso ocorre por meio da solicitação de senhas, logins ou biometria.

A presente política será executada pelos seguintes meios:

(13) 3343-9050
@guarujaprevidencia
@guarujaprevidencia
guarujaprevidencia.sp.gov.br
Av. Adhemar de Barros, 230 - Bairro Santo Antônio
Guarujá/SP - CEP 11430 - 000

- **Informativo:** Divulgar essa política e esclarecer dúvidas; notificar as pessoas sobre ações que não estão em conformidade com esta política e informar as autoridades competentes sobre ocorrências;

- **Delimitativo:** Discriminar os direitos e limitações sobre a utilização dos recursos de TI;

- **Ação:** Disponibilizar recursos com segurança, monitorar, aplicar ações corretivas e comunicar autoridades competentes.

2.2 Abrangência - A quem se destina esta política

A Política de segurança da informação da GuarujáPrev aplica-se a todos os servidores ativos do quadro de funcionários e prestadores de serviços. Esta política aplica-se também aos trabalhos executados fora das dependências da autarquia ou que utilizem recursos de tecnologia da informação e dados de propriedade da Guarujá Previdência.

Todo e qualquer usuário de recursos de Tecnologia de Informação (TI) da GuarujáPrev tem a responsabilidade de proteger a segurança e a integridade das informações e dos equipamentos de informática.

É dever de todos da GuarujáPrev considerar a informação como sendo um bem de grande valor da organização, um recurso crítico e necessário para a boa condução da autarquia e que deve sempre ser utilizado de forma profissional.

3. TRATAMENTO DA INFORMAÇÃO

3.1 Classificação e guarda da informação

É importante que se tenha preocupação em organizar a informação gerada como um processo de trabalho contínuo para que se tenha disponibilidade para os envolvidos, para que se transmita para quem é de direito e para que se mantenha enquanto necessária.

É de responsabilidade do Gerente/Responsável de cada área estabelecer critérios relativos ao nível de confidencialidade da informação gerada por sua área de acordo com as seguintes classificações:

a. **Pública:** é toda informação que pode ser acessada por usuários da autarquia, pessoas externas, fornecedores, prestadores de serviços e público em geral.

(13) 3343-9050
@guarujaprevidencia
@guarujaprevidencia
guarujaprevidencia.sp.gov.br
Av. Adhemar de Barros, 230 - Bairro Santo Antônio
Guarujá/SP - CEP 11430 - 000

b. **Interna:** é toda informação que só pode ser acessada por colaboradores da organização. São informações que possuem um grau de confidencialidade que pode comprometer a imagem da autarquia.

c. **Confidencial:** É toda informação que pode ser acessada por usuários da organização e por parceiros da organização. A divulgação não autorizada dessa informação pode causar impacto (financeiro, de imagem ou operacional) nas atividades da Autarquia ou ao negócio do parceiro.

d. **Restrita:** É toda informação que pode ser acessada somente por usuários da organização explicitamente indicados pelo nome ou por área a que pertence. A divulgação não autorizada dessa informação pode causar sérios danos ao cumprimento dos objetivos da autarquia e/ou comprometer a estratégia e a condução da organização.

3.1.1 Responsabilidades

Todo Gerente/Responsável de cada setor deve:

- orientar seus subordinados a não circularem informações e/ou mídias consideradas confidenciais e/ou restritas,
- não deixar relatórios nas impressoras e mídias em locais de fácil acesso, tendo sempre em mente o conceito “mesa limpa”, ou seja, ao terminar o trabalho não deixar nenhum relatório e/ou mídia confidencial e/ou restrito sobre suas mesas.
- classificar a informação de acordo com seu processo produtivo, devendo entregar ao seu superior ou ao setor de TI a documentação contendo o descritivo dos seguintes itens:

  1. Quais informações precisam ser guardadas;

  2. Resumo do assunto, informando qual o processo está sendo controlado/produzido com essa informação;

  3. Temporalidade para a guarda, com estimativa do prazo de retenção. Podendo ser uma data, um prazo ou um vínculo com um processo em que a informação é utilizada;

  4. Informar se a informação deve ser eliminada ou arquivada quando chegar o fim de sua temporalidade;

(13) 3343-9050
@guarujaprevidencia
@guarujaprevidencia
guarujaprevidencia.sp.gov.br
Av. Adhemar de Barros, 230 - Bairro Santo Antônio
Guarujá/SP - CEP 11430 - 000

5. Em caso da digitalização de arquivo, deve ser verificado se este foi processado da forma mais adequada visando obter a melhor qualidade da informação ao custo de menor tamanho possível levando em conta a sua utilidade.

Após este procedimento, a informação será considerada organizada, relevante para a autarquia e deve estar facilmente acessível para os envolvidos.

3.2 Tratamento dos dados pessoais de colaboradores, servidores e de terceiros

A autarquia compromete-se a não acumular ou manter intencionalmente dados pessoais além daqueles relevantes a realização de suas atividades. Todos os dados pessoais serão considerados confidenciais. Dados pessoais sob a responsabilidade da autarquia não serão usados para fins

diferentes daqueles para os quais foram coletados. Dados pessoais não serão transferidos para terceiros, exceto quando autorizados, devendo seus receptores manterem a confidencialidade, incluindo-se, neste caso a lista de endereços eletrônicos (e-mails) usados pelos servidores da GUARUJÁ PREVIDÊNCIA.

3.3 Aquisição e adaptação de programas de computador

Ao se detectar a necessidade de utilizar um programa de computador para uma finalidade, o setor de TI ou o responsável pelo setor que utilizará o programa, deverá estar ciente sobre essa utilização e ser consultado sobre possíveis alternativas e forma de aquisição de licenças de software.

A instalação de programas deverá ser feita utilizando-se de arquivos de fontes confiáveis e a aquisição dos arquivos de instalação deverá ser feita preferencialmente através dos fornecedores oficiais, independentemente do tipo de licença de uso do aplicativo em questão, seja de origem gratuita, proprietária ou governamental.

Devem ser evitados sites de publicidade de programas, que embutem programas desnecessários aos instaladores ou outras fontes de instaladores duvidosos. Estes sites podem ser usados somente para consulta.

(13) 3343-9050
@guarujaprevidencia
@guarujaprevidencia
guarujaprevidencia.sp.gov.br
Av. Adhemar de Barros, 230 - Bairro Santo Antônio
Guarujá/SP - CEP 11430 - 000

Recomenda-se, em todos os casos, a guarda dos dados em local seguro e a utilização de ambiente de teste para instalações de programas de origem ainda desconhecida por quem irá fazer a instalação, mesmo que a fonte de obtenção do software seja oficial.

O setor de TI não se opõe que usuários façam instalações de programas diversos e configurações para auxílio nos trabalhos de cada setor, desde que o usuário tenha conhecimento sobre os procedimentos técnicos e responsabilidades sobre possíveis consequências, que podem inclusive impactar seu trabalho e de outros utilizadores da rede.

Ocorrências podem ocasionar no desperdício de mão-de-obra para resolução de incidentes emergenciais.

Recomenda-se que o setor de TI seja informado, bem como os responsáveis de cada setor a respeito de quais programas são utilizados para produzir informação relevante e que haja o controle da informação organizada de forma a permitir a boa definição dos processos e sua reprodução por outros colaboradores.

3.4 Utilização de recursos de TI

São recursos de TI qualquer equipamento, objeto ou método capaz de reter ou transmitir informação, como exemplo:

- Computadores Desktop, notebook;
- Periféricos: teclado, mouse, impressora, câmeras, gravadores de áudio, etc.;
- Dispositivos de armazenamento e suas mídias;
- Equipamentos de rede, servidores;
- Equipamentos de telecomunicação pessoal: telefone, smartphone, rádio;
- Programas de computador e sistemas;
- Impressos e anotações;
- Os procedimentos adotados para a aquisição da informação;
- Serviços de telecomunicações como telefonia e internet;
- A própria informação.

(13) 3343-9050
@guarujaprevidencia
@guarujaprevidencia
guarujaprevidencia.sp.gov.br
Av. Adhemar de Barros, 230 - Bairro Santo Antônio
Guarujá/SP - CEP 11430 - 000

3.4.1 Sobre a disponibilização de recursos de TI:

Os recursos de tecnologia da informação, disponibilizados para os usuários, têm como objetivo prioritário a realização de atividades profissionais;

A proteção do recurso de TI de uso individual é de responsabilidade do próprio usuário;

É de responsabilidade de cada usuário assegurar a integridade do equipamento, a confidencialidade e disponibilidade das informações contidas nele;

As comunicações devem ser escritas em linguagem profissional, não devem comprometer a imagem da autarquia, não podem ser contrárias à legislação vigente e nem aos princípios éticos da Guarujá Previdência;

É permitido aos colaboradores a utilização de recursos de TI de propriedade particular para fins profissionais se assim acharem conveniente desde que:

- Exista total aderência e atenção a esta política de segurança em todos os seus termos;
- Inicialmente, o colaborador fique responsável por garantir todos os requisitos desta política nos recursos fornecidos, sendo responsável por exposição de vulnerabilidades de segurança ocorridas;
- O setor de TI seja comunicado sobre a utilização;
- Haja separação de conteúdo pessoal e profissional;
- O conteúdo pessoal não infrinja a normas dessa política;
- Enquanto em utilização do recurso para fins profissionais, todas as proibições se aplicam ao recurso particular.

É permitida a utilização de recursos de TI de propriedade da autarquia para fins pessoais, desde que fora do horário de expediente nos seguintes termos:

- A utilização não pode expor o recurso a vulnerabilidades de segurança e não pode desrespeitar as normas desta política;
- O recurso utilizado não pode ser um consumível que gere custo considerável para a autarquia;
- O recurso não pode sofrer configurações ou adaptações para atender a necessidades pessoais que sejam diferentes das necessidades profissionais;
- Não é permitida a configuração ou modificação de qualquer recurso de TI da Autarquia para fins de entretenimento assim como instalação de recursos adicionais aos recursos cedidos pela Guarujá Previdência para alcançar tal finalidade.

(13) 3343-9050
@guarujaprevidencia
@guarujaprevidencia
guarujaprevidencia.sp.gov.br
Av. Adhemar de Barros, 230 - Bairro Santo Antônio
Guarujá/SP - CEP 11430 - 000

3.4.2 Proibições na utilização de recursos de TI

É proibida a utilização de qualquer recurso de TI para guardar ou transmitir informação confidencial e restrita de propriedade da GuarujáPrev de forma que possibilite acesso a pessoas não autorizadas. Informações públicas e internas devem ser elaboradas, revisadas e validadas de ofício por pessoa competente, a fim de evitar divergências, especulações, perda da qualidade da informação e retrabalho, sendo vedada a utilização de recursos de TI para transmissão de informações não preparadas para tal finalidade.

É proibido utilizar recursos de TI de propriedade da autarquia ou particular para gerar, executar automações, pesquisar, obter e compartilhar conteúdo dos seguintes gêneros:

• Que defendam atividades ilegais;

• Que menosprezem, depreciem ou incitem preconceito de qualquer natureza;

• Conteúdo pornográfico ou relacionado a sexo;

• Declarações difamatórias e linguagem ofensiva;

• Que possam trazer prejuízos de forma ilegal a outras pessoas;

• Conteúdos hostis e inúteis;

• “Correntes” ou equivalentes;

• Que prejudiquem a imagem da organização;

• Que prejudiquem a imagem de outras organizações;

• Que sejam incoerentes com as políticas da GUARUJÁ PREVIDÊNCIA;

• Que explorem vulnerabilidades de segurança de qualquer espécie, exceto se efetuada por profissional autorizado;

• Que possuam origem duvidosa ou que possam causar danos a algum recurso.

3.4.3 Utilização dos recursos de TI fora do local de trabalho

• Mantenha o equipamento sempre com você;

• Tenha atenção em hall de hotéis, aeroportos, aviões, táxi etc.

• Utilize sempre o porta-malas ou lugar não visível para o transporte do equipamento em automóvel;

(13) 3343-9050
@guarujaprevidencia
@guarujaprevidencia
guarujaprevidencia.sp.gov.br
Av. Adhemar de Barros, 230 - Bairro Santo Antônio
Guarujá/SP - CEP 11430 - 000

• Tenha atenção ao transportar o equipamento na rua.

Em caso de furto:

• Registre a ocorrência em uma delegacia de polícia;

• Comunique ao seu superior imediato e ao Setor de TI;

3.4.4 Monitoramento, controle e auditoria de acesso

Em momento oportuno, para garantir a qualidade dos recursos de TI, o setor de TI, dentro de suas possibilidades, se reserva ao direito de:

- Monitorar o armazenamento e transmissão de dados, vídeo e voz, através de meios de qualquer espécie, seja de recursos de TI de propriedade da Autarquia 24 horas por dia ou de propriedade particular quando em uso em local/horário de trabalho, independente se forem utilizados para fins pessoais ou profissionais;
- Registrar e gerar relatórios de acesso a todos os tipos de informações e recursos de TI da Guarujá Previdência;
- Bloquear a transmissão de dados de aplicativos diversos;
- Bloquear usuários com padrão de utilização prejudicial a algum recurso;
- Desinstalar aplicativos em computadores através de acesso remoto ou local;
- Desativar qualquer dispositivo ou equipamento com comportamento que prejudique a integridade dos demais recursos;
- Emitir relatório com parecer técnico para superior hierárquico e/ou autoridade para providenciar medidas cabíveis.
- Promover ações de conscientização sobre segurança da informação.

3.5 Permissões e senhas

O setor de Gestão de Pessoas da Guarujá Previdência deverá informar ao setor de TI toda e qualquer movimentação, admissão e demissão de colaboradores para que possam ser cadastrados ou excluídos no sistema da autarquia. Isto inclui o fornecimento de sua senha e registro do seu nome como usuário em sistemas, pelo setor de TI. Cabe ao setor de origem do novo usuário a comunicação ao setor de TI sobre as rotinas a que o novo contratado terá direito de acesso e quais serão restritas. Nenhum colaborador poderá ter acesso a qualquer recurso de TI sem ter

(13) 3343-9050
@guarujaprevidencia
@guarujaprevidencia
guarujaprevidencia.sp.gov.br
Av. Adhemar de Barros, 230 - Bairro Santo Antônio
Guarujá/SP - CEP 11430 - 000

expressamente concordado com esta política. Recomenda-se cuidado e sigilo sobre a guarda de nome de usuários e senhas. Estas informações fazem parte do grupo de dados que é utilizado para rastrear incidentes de segurança que possam ocorrer em sistemas diversos e rede. Tais incidentes podem ocasionar sanções caso ocorra prejuízos à segurança das informações da autarquia.

3.6 Pastas compartilhadas e cópia de segurança e rotinas de recuperação de desastres

Deverá haver levantamento constante de cada setor da autarquia sobre documentos relevantes e organizados que serão armazenados. Este armazenamento poderá ser em pastas departamentais, de processos ou públicas e poderão ser compartilhadas pela rede conforme necessidade.

O setor de TI deve receber cópia dos arquivos compartilhados para que possa efetuar backup periódico e evitar potenciais perdas de informação para a Autarquia. É de responsabilidade dos próprios usuários a elaboração de cópias de segurança dos arquivos em suas estações de trabalho.

Os arquivos que não fazem parte dos processos de negócio da autarquia podem ser compartilhados entre os colaboradores, mas não serão objeto de armazenamento em servidor centralizado ou de backup periódico.

3.7 Segurança de sistemas e bancos de dados

O gerenciamento do(s) banco(s) de dados é responsabilidade do setor de TI e seus fornecedores contratados, assim como a manutenção, alteração e atualização de equipamentos, softwares e a guarda de backups.

3.8 Plano de Contingência

Contingência é a situação de incerteza quanto a um determinado evento, fenômeno ou acidente, que pode se concretizar ou não, durante um período determinado.

O plano de contingência da Guarujá Previdência tem o objetivo de descrever as medidas a serem tomadas pela autarquia, no caso da ocorrência de um evento indesejável, que afete ou possa afetar negativamente seus processos.

Visa estabelecer uma estrutura de responsabilidade para tomada de decisão durante uma emergência e procedimento que permitam agilizar as ações com eficácia em qualquer ponto das

(13) 3343-9050
@guarujaprevidencia
@guarujaprevidencia
guarujaprevidencia.sp.gov.br
Av. Adhemar de Barros, 230 - Bairro Santo Antônio
Guarujá/SP - CEP 11430 - 000

instalações, reduzindo ao mínimo o perigo potencial de lesões, mortes, prejuízos, danos a propriedade, ao meio ambiente e a toda coletividade.

3.8.1 Etapas do Plano de Contingência

O Plano de Contingência foi desenvolvido para ser acionado quando da ocorrência de cenários que apresentam risco à continuidade dos serviços essenciais.

Ações de pessoas que possam gerar incidentes cotidianos e de baixa gravidade serão tratados com medidas informativas e corretivas.

Ações que possam causar incidentes graves podem gerar punições administrativas e enquadramentos em infrações legais.

O quadro abaixo define estes riscos e aponta quais parâmetros para reportar as possíveis causas da ocorrência:

EVENTOS / IDENTIFICAÇÃO DO RISCO	POSSÍVEIS CAUSAS /AVALIAÇÃO DO RISCO	ESTRATÉGIA / AÇÕES
01- Interrupção de energia elétrica	Causada por fator externo à rede elétrica do prédio ou de sua localidade com duração da interrupção superior a 30 minutos. Causada por fator interno que comprometa a rede elétrica do prédio com curto-circuito, incêndio e infiltrações.	Se a falta de energia for de curta de duração, máximo 30 minutos, os sistemas e servidores de rede continuam em funcionamento, pois estão ligados em um nobreak. Caso a falta de energia dure mais de 30 minutos, os sistemas são desligados, bem como os equipamentos e serão religados assim que a energia for reestabelecida.
02- Falha na climatização do servidor	Superaquecimento dos ativos devido a falha no sistema de climatização	Readequação das divisórias da copa para abrigar o espaço para o servidor de rede. Deverá ter monitoramento de temperatura e desativação dos ativos caso o problema de climatização dure vários dias.
03 - Indisponibilidade de rede/circuitos	1-Rompimento de cabeamento decorrente de execuções obras internas, desastres ou acidentes.	1- Será verificado se cabeamento pertence à autarquia ou prestador de serviço. Sendo de prestador de serviço, este será comunicado para efetuar reparo urgente. Caso seja da autarquia, a equipe interna efetuará o reparo.
04 - Falha humana	Acidente ao manusear equipamentos / sistemas	Atualmente, todos os ativos de TI possuem de alguma forma, possibilidade de substituição. Sempre há trabalho contínuo

(13) 3343-9050
@guarujaprevidencia
@guarujaprevidencia
guarujaprevidencia.sp.gov.br
Av. Adhemar de Barros, 230 - Bairro Santo Antônio
Guarujá/SP - CEP 11430 - 000

		visando garantir equipamentos sobressalentes visando manter os serviços contínuos. Primeiramente será avaliado possibilidade de reparo e se o tempo necessário for menor que a disponibilização de ativo de substituição, as áreas afetadas deverão aguardar o reparo. Em segundo caso, será configurado novo ativo visando atender a pessoa ou grupo atingido pelo incidente. São feitas cópias de arquivos em nuvem, visando restaurar arquivos, incluindo dados históricos de configurações de sistemas, equipamentos de rede, base de dados e arquivos de documentos pessoais e departamentais.
05 - Ataques internos (usuários insatisfeitos)	Ataque aos ativos e equipamentos de TI e de uso administrativo	Será avaliado se deverá haver reparo ou substituição, similar ao item anterior (04).
06- Falha de hardware	Falha que necessite reposição de peça ou reparo cujo reparo ou aquisição dependa de processo licitatório	As aquisições de equipamentos são feitas visando possuir equipamento sobressalente. Peças de reposição podem ser feitas com dispensa de processo licitatório em emergências.
07- Ataque cibernético	Ataque virtual que comprometa o desempenho, os dados ou configuração dos serviços essenciais	Cópias de segurança do sistema integrado e dos servidores de rede são de responsabilidade da TI e deverão ser feitas periodicamente. Cada tipo de sistema deve possuir medidas de evitar invasão, como configurações de bloqueio a acessos desnecessários, atualização de segurança e programa de monitoramento de risco de segurança.
08 - Problemas de conexão com a internet	Falhas e bugs temporários da conexão; flutuações inesperadas no uso; vírus nos dispositivos; tipo de banda larga; roteador de baixa qualidade ou antigo; dispositivos longe do roteador	1. Identificar em qual área está ocorrendo o problema; 2. Analisar a conexão do servidor central; 3. Identificar a causa do problema; 4. Detectado problema externo de internet, ativar o link de internet de contingência; 5. Abrir chamado de suporte com a operadora, visando o reestabelecimento do serviço.
09 - Outros Problemas	Configurações de e-mail, impressoras, problemas de acesso que envolvam login e senha e etc	Para qualquer outro tipo de problema que envolva a TI, como configurações de e-mail, impressoras, problemas de acesso que envolvam login e senha etc.

(13) 3343-9050
@guarujaprevidencia
@guarujaprevidencia
guarujaprevidencia.sp.gov.br
Av. Adhemar de Barros, 230 - Bairro Santo Antônio
Guarujá/SP - CEP 11430 - 000

		Os passos a serem seguidos são os seguintes: 1. Informar o problema ao Setor de TI do - O atendimento será priorizado conforme gravidade da demanda e devidamente agendado; 2. Após o atendimento, o solicitante é informado da conclusão/resolução do problema reclamado;

4. Propriedade intelectual

É de propriedade da Guarujá Previdência, todos os projetos, criações ou procedimentos desenvolvidos por qualquer colaborador durante o curso de seu vínculo com a autarquia. É permitida a recriação ou reprodução de projeto ou peça similar desde que não seja constatada cópia de conteúdo ou utilização de dados sigilosos.

5. Violações da Política de Segurança da Informação e disposições finais

Implicam em violação desta política de segurança da informação, qualquer ato que:

a) Envolva a revelação de dados confidenciais;
b) Exponha dados ainda não tratados ou divergentes;
c) Faça uso não autorizado de dados da organização;
d) Exponha a Autarquia a uma possível perdas de qualquer natureza por meio da exposição de informações;
e) Exponha a Autarquia a quaisquer perdas por motivo de mau uso ou guarda indevidos de recursos de tecnologia da informação;
f) Envolva o uso de dados para propósitos ilícitos, que venham a violar qualquer lei, regulamento ou outro dispositivo normativo.

Esta política permanece aplicável ao servidor e terceiros após seu desligamento enquanto forem responsáveis pelos seus atos administrativamente e criminalmente.

(13) 3343-9050
@guarujaprevidencia
@guarujaprevidencia
guarujaprevidencia.sp.gov.br
Av. Adhemar de Barros, 230 - Bairro Santo Antônio
Guarujá/SP - CEP 11430 - 000

Ao tomar ciência desta política, todos concordam em não divulgar dados sensíveis a que tiverem acesso, seja por meios lícitos ou não, bem como garantir a guarda das informações confiadas.

6. CONTROLE DE VERSÕES:

Elaborado por	Revisado por	Aprovado por	Versão	Data da ovação
Analista Previdenciário de Suporte	Analista Previdenciário de Controle Interno	Gerente de ministração	1.0	15/12/2016
Sávio Sabino Analista Previdenciário de Suporte 01/04/2022	Luciana Marin Faneco Analista Previdenciário de Controle Interno 04/04/2022	Maria José Lima Rodrigues Gerente de Administração	2.0	12/04/2022 *assinatura eletrônica)*