INOVAR PREVIDÊNCIA

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

APROVADO EM REUNIÃO DO CONSELHO DELIBERATIVO DE 30 DE JUNHO DE 2022

SUMÁRIO

1. APRESENTAÇÃO

As informações da Inovar Previdência - Sociedade de Previdência Privada ("Inovar Previdência" ou "Entidade"), de natureza técnica, operacional, comercial ou de qualquer forma relacionada as suas atividades como Entidade Fechada de Previdência Complementar, de seus patrocinadores, instituidores e prestadores de serviços (em conjunto, "Informações"), bem como os dados pessoais de seus participantes, assistidos, beneficiários, colaboradores, representantes de prestadores de serviços e/ou usuários do portal institucional, dentre outros (em conjunto, "Dados Pessoais") são ativos que requerem proteção e tratamento de forma ética e sigilosa, de acordo com a legislação vigente e as normas internas da Entidade, evitando-se o mau uso, a perda e a exposição indevida.

O efetivo cumprimento desta Política de Segurança da Informação ("Política") é uma importante ferramenta para combater ameaças a estes ativos, sob gestão e controle da Inovar Previdência, bem como para prever a responsabilidade legal em caso de descumprimento.

A observância dessa Política é fundamental, ainda, para cumprimento das disposições da legislação de proteção de dados vigente no país, em especial, a Lei nº 13.709/2018 ("Lei Geral de Proteção de Dados Pessoais" ou "LGPD") no que se refere a segurança e sigilo dos Dados Pessoais e deverá ser cumprida, conjuntamente, com a Política de Privacidade da Inovar Previdência, disponível no portal institucional da Entidade.

2. OBJETIVO

Esta Política é um conjunto de diretrizes que visa conscientizar e orientar os colaboradores da Inovar Previdência e seus prestadores de serviços para o uso seguro das Informações e Dados Pessoais, garantindo a observância aos princípios inerentes à Segurança da Informação, quais sejam:

- Integridade: salvaguarda da exatidão e correção da informação, bem como dos métodos de processamento;
- Confidencialidade: propriedade que garante que a informação seja acessada somente pelas pessoas ou processos que tenham autorização para tal;
- Disponibilidade: propriedade da informação estar acessível e utilizável sempre que necessário;
- Autenticidade: garantia de que seja identificado e registrado o usuário que está enviando ou modificando a informação.

As orientações aqui apresentadas são os princípios fundamentais e representam como a Inovar Previdência exige que as Informações e os Dados Pessoais sejam utilizados.

Os princípios relacionados à proteção dos Dados Pessoais como a boa-fé, finalidade, adequação, necessidade, dentre outros elencados na Lei Geral de Proteção de Dados Pessoais deverão ser, igualmente, observados no cumprimento desta Política.

Esta Política se aplica para o que está armazenado em ambiente tecnológico, ou seja, nos computadores, redes ou sistemas utilizados pela Inovar Previdência e, também, para os documentos físicos impressos que contenham Informações e/ou Dados Pessoais.

3. ABRANGÊNCIA

Esta Política se aplica a todos os colaboradores da Inovar Previdência, bem como seus prestadores de serviços que eventualmente tenham acesso aos recursos tecnológicos e documentos da Entidade que contenham Informações e/ou Dados Pessoais.

É obrigação de cada colaborador se manter atualizado em relação a esta Política e aos procedimentos e normas a ela relacionadas, buscando orientação do seu gestor, da área de *compliance* ou do suporte de TI contratado sempre que não estiver seguro quanto às diretrizes aqui apresentadas.

Não é escusável o descumprimento da Política, alegando desconhecimento, devendo observar integralmente o que dispõe este documento. A inobservância destas regras acarretará a apuração das responsabilidades funcionais previstas no contrato de trabalho e seus anexos, normativos internos e na legislação em vigor, podendo haver responsabilização penal, civil e administrativa. O cumprimento da Política poderá ser auditado pela Inovar Previdência.

Esta Política dá ciência a cada colaborador e prestadores de serviços que os ambientes, sistemas, computadores e redes da Entidade poderão ser monitorados e gravados, com prévia informação, conforme previsto nas leis brasileiras.

4. DIRETRIZES PARA SEGURANÇA DA INFORMAÇÃO

Esta Política define as Diretrizes para a Segurança da Informação, visando preservar a integridade, confidencialidade, autenticidade e disponibilidade dos ativos sob gestão da Inovar Previdência. Descreve a conduta considerada adequada para o manuseio, controle das Informações e Dados Pessoais contra acessos não autorizados, destruição, modificação e divulgação indevida, seja acidental ou intencionalmente.

4.1. Propriedade das informações

Toda Informação produzida, acessada, recebida, manuseada ou armazenada pelos colaboradores, como resultado da atividade profissional, bem como, a reputação, a marca e demais ativos são de propriedade e de direito de uso exclusivos da Inovar Previdência, sendo, portanto, proibidas as cópias, reproduções ou distribuições sem a devida autorização. As exceções devem ser explícitas e formalizadas pela Entidade.

A utilização da marca, identidade visual e demais sinais distintivos da Inovar Previdência, em qualquer veículo de comunicação, inclusive na Internet e nas mídias sociais, só poderão ser feitos para atender às atividades profissionais da Entidade.

4.2. Classificação das Informações

É de responsabilidade de cada gestor estabelecer critérios relativos ao nível de confidencialidade da informação gerada ou recebido por sua área, de acordo com os critérios a seguir:

a) **Pública:** Informações da Entidade com linguagem e formato dedicado à divulgação ao público em geral, sendo de caráter informativo, comercial ou promocional. É destinada ao público externo ou ocorre devido ao cumprimento de legislação;

b) **Corporativa:** Informações cujo conhecimento é de interesse de toda Entidade, podendo ser divulgada para beneficiários, participantes e parceiros;

c) **Uso Interno:** Informações de conhecimento exclusivo dos colaboradores da Entidade e deve ser divulgada apenas para o público interno;

d) **Restrita:** É toda informação que pode ser acessada somente por colaboradores de áreas previamente definidas em manual específico;

e) **Confidencial:** É uma informação crítica para os negócios da Entidade ou de parceiros, devendo haver indicação do nome ou cargo do colaborador responsável. A divulgação não autorizada dessa informação pode causar impactos de ordem financeira, de imagem, operacional ou, ainda, sanções administrativas, civis e/ou criminais.

Nenhuma das Informações restritas ou confidenciais podem ser repassadas para terceiros sem consentimento formalizado da Inovar Previdência.

4.3. Propriedade e Classificação dos Dados Pessoais

Os Dados Pessoais pertencem à pessoa natural a quem se referem as informações, na condição de titulares de Dados Pessoais. Todos seus direitos são previstos e assegurados pela Lei Geral de Proteção de Dados Pessoais e deverão ser observados pela Entidade durante o tratamento, em consonância com a Política de Privacidade da Inovar Previdência.

Os Dados Pessoais deverão sempre serem classificados como restritos e confidenciais, não podendo serem repassados para terceiros sem que haja a devida hipótese legal da Lei Geral de Proteção de Dados Pessoais que o autorize: consentimento, cumprimento de obrigação legal ou regulatória, execução do contrato, proteção de crédito e/ou legítimo interesse.

4.4. Utilização, Guarda e Descarte de documentos físicos

Documentos que contenham Informações classificadas como uso interno, restrita ou confidencial e/ou Dados Pessoais não podem ficar expostos na estação de trabalho, em impressoras, *scanner*, telas de computadores, áreas comuns, locais de trânsito de pessoas, refeitório e nas salas de reunião.

Referidos documentos físicos devem ser acondicionados em armários, o qual seja garantida a devida segurança com chaves. Igualmente, deve-se garantir o zelo na contratação e renovação dos contratos de prestadores de serviço para armazenamento de documentos físicos.

Deve-se observar a exigência e o prazo legal definido em tabela vigente à época, para manutenção dos documentos produzidos em razão de suas atividades. Decorrido o prazo para armazenamento, os documentos devem ser destruídos antes de descartados, mediante autorização prévia do gestor responsável.

4.5. Boas Práticas para impressões

Com relação aos documentos enviados para impressão, estes deverão ser recolhidos imediatamente das impressoras pelo responsável após sua impressão, caso a impressora não possua o recurso de impressão por crachá, em especial, aqueles que contenham Informações restritas ou confidenciais e/ou Dados Pessoais.

4.6. *Backup* (Cópias de segurança)

Os *backups* devem ser realizados por sistemas de agendamento e executados, preferencialmente, fora do horário comercial, período em que não há nenhum ou pouco acesso de usuários ou processos automatizados dos sistemas de informática.

Os prestadores de serviços contratados e/ou colaboradores responsáveis pela gestão dos sistemas de *backup* deverão realizar pesquisas frequentes para identificar atualizações de correção, novas versões do produto, ciclo de vida, sugestões de melhorias, entre outros.

A rotina implementada de *backup* deve estar formalmente documentada para consultas e auditorias.

4.7. Segurança do Ambiente Físico

É vedado o acesso de pessoas não autorizadas às instalações da Inovar Previdência. O acesso de visitantes ou prestadores de serviços deverá ser supervisionado por gestor ou colaborador da Entidade, com exceção de pessoas e equipes previamente autorizadas pela Inovar Previdência.

É fundamental que, durante a jornada de trabalho e nas dependências da Inovar Previdência, os colaboradores utilizem crachá de identificação. O acesso de informações restritas ou confidenciais devem ser controladas por meio de detenção de chaves para acesso dos armários.

O acesso aos locais de desenvolvimento de atividades da Entidade com quaisquer equipamentos de gravação, fotografia, vídeo, som ou outro tipo de equipamento similar, para fins de gravação dos ambientes de trabalho, somente poderá ser realizado a partir de autorização da Inovar Previdência e mediante supervisão.

Não é permitido aos colaboradores tirar fotos, gravar, filmar, publicar elou compartilhar imagens dos locais de desenvolvimento de atividades da Inovar Previdência que possam:

a) Comprometer a segurança dos demais colaboradores;

b) Comprometer o sigilo das Informações e Dados Pessoais;

c) Comprometer os direitos dos titulares de Dados Pessoais, no que tange, a Dados Pessoais Sensíveis relacionados a fotos e biometria;

d) Impactar negativamente a imagem da Inovar Previdência, outros colaboradores, clientes, parceiros e/ou visitantes.

4.8. Mesa Limpa/Tela Limpa

Deve ser seguido pelos colaboradores da Inovar Previdência o princípio estabelecido na Norma ABNT NBR/ISO/IEC 27.001 da "Mesa limpa/Tela limpa". Este princípio tem como objetivo a redução dos riscos de acesso não autorizado, perda de informações ou danos às informações durante e fora do horário de expediente.

A política de "Mesa Limpa/Tela Limpa" busca resguardar a Inovar Previdência contra acessos não autorizados a Informações e Dados Pessoais. Assim, sinteticamente, entre outros:

a) Papéis, anotações e lembretes devem ser mantidos, sempre que possível, fora da superfície da mesa (mesa limpa);

b) Informações restritas ou confidenciais e/ou Dados Pessoais devem ser alocadas com segurança; (idealmente em um arquivo, armário ou gaveteiro)

c) Computadores e *notebooks* não devem ser deixados autenticados/registrados quando não houver um colaborador junto e devem ser protegidos por senhas e outros controles quando não estiverem em uso (tela limpa);

d) Utilização de protetor de tela que solicite uma senha para acesso deve ser sempre usado;

e) Informações restritas ou confidenciais e/ou Dados Pessoais, quando impressos, devem ser retiradas da impressora imediatamente pelo colaborador que solicitou a impressão;

f) Ao final do dia, ou no caso de ausência prolongada, a mesa de trabalho deve ser limpa; e

g) Todos os documentos e meios eletrônicos, no final do dia de trabalho, devem ser devidamente guardados/organizados, com proteção adequada.

4.9. Utilização dos Equipamentos de Informática e Comunicação

A cada colaborador é disponibilizado pela Inovar Previdência os próprios equipamentos de informática para desenvolvimento das suas atividades profissionais. Excepcionalmente, o uso pessoal dos recursos é permitido desde que não prejudique o desempenho dos sistemas e serviços.

A Inovar Previdência poderá registrar todo e qualquer uso dos sistemas e serviços, visando garantir a disponibilidade e a segurança das Informações e Dados Pessoais. A responsabilidade em relação à Segurança da Informação será comunicada na fase de contratação dos colaboradores, os quais deverão assinar um termo de responsabilidade.

O uso de aparelhos de comunicação pessoais fica autorizado, enquanto não há aprovação para disponibilização de aparelhos institucionais, de modo a não impedir ou prejudicar as atividades desenvolvidas pelo colaborador. Deverão ser observadas as mesmas regras de segurança, contidas nesta Política, durante o uso de aparelhos de comunicação pessoais.

4.10. Controles de Acesso/*Logins*

Para cada colaborador da Inovar Previdência deverá ser fornecido dispositivos de identificação pessoal, como crachá, códigos de acesso e senhas, os quais, não poderão ser compartilhados, divulgados ou transferidos a outra pessoa. O colaborador é responsável por todas as atividades desenvolvidas por meio de seus dispositivos de identificação pessoal. É vedada, a qualquer colaborador, a utilização de dispositivos de identificação pessoal de outro colaborador mesmo quando cedida por este.

É de responsabilidade de cada colaborador da Entidade a guarda dos dispositivos de identificação que lhe forem designados, bem como, a memorização de sua própria senha, não devendo anotar ou armazená-las em arquivos eletrônicos sem utilizar um meio de proteção definido pelo suporte de TI, como, por exemplo, criptografia.

As senhas não devem ser baseadas em informações pessoais, como o próprio nome, nome de familiares, data de nascimento, endereço, placa de veículo, nome da Entidade, nome do departamento e não devem ser constituídas de combinações óbvias de teclado, como "abcdefgh", "87654321", entre outras. As senhas de acesso deverão ser trocadas ao menos semestralmente.

Se existir *login* de uso compartilhado por mais de um colaborador, a responsabilidade perante a Entidade e a legislação (civil e criminal) será dos colaboradores que dele se utilizarem.

A concessão de acessos pelos gestores deverá seguir o critério de menor privilégio, no qual os colaboradores tenham acesso apenas às Informações e Dados Pessoais imprescindíveis para o pleno desempenho de suas atividades.

Os gestores das áreas da Entidade deverão, através de e-mail, solicitar ao suporte de TI e provedores de sistemas inclusões, alterações ou exclusões de acesso a usuários, definindo os serviços que deverão ser incluídos, alterados ou excluídos e justificando quanto à necessidade da solicitação.

Todos os acessos devem ser imediatamente bloqueados quando se tornarem desnecessários. Portanto, por ocasião do desligamento de qualquer colaborador, os gestores responsáveis deverão solicitar o imediato cancelamento de todas as suas senhas de acesso a equipamentos e sistemas corporativos bem como de seu e-mail.

As autorizações devem ser revistas, confirmadas e registradas continuadamente. O responsável pela autorização ou confirmação da autorização deve ser claramente definido e registrado.

4.11. Segurança dos Equipamentos e Instalação de *Softwares*

É proibido todo procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação, sem o conhecimento prévio e o acompanhamento do gestor responsável e suporte de TI contratado, exceto naqueles *softwares* e aplicações que necessitam de atualização para sua devida utilização.

Não é permitida a alteração da configuração dos sistemas operacionais dos equipamentos, em especial, os referentes à segurança e à geração de *logs*, sem a devida comunicação e a autorização da área responsável e sem a condução, auxílio ou presença do suporte do TI contratado.

O usuário é proibido de remover toda e qualquer versão de *software* obsoleto, mesmo em casos onde exista uma versão atualizada da aplicação utilizada. Caso o usuário necessite instalar ou remover qualquer *software*, deverá entrar em contato com o gestor responsável.

Não é permitida a instalação/uso de *softwares* ilegais (sem licenciamento), sendo que o suporte de TI poderá valer-se desta Política para desinstalar, sem aviso prévio, todo e qualquer *software* sem licença de uso, em atendimento à Lei 9.609/98 (Lei do *Software*).

É proibido executar programas, instalar equipamentos, armazenar arquivos ou promover ações que possam facilitar o acesso de usuários não autorizados à rede corporativa da Inovar Previdência.

O colaborador deverá responsabilizar-se em não utilizar quaisquer programas e/ou aplicativos, inclusive gratuitos, que não tenham sido instalados ou autorizados pelo suporte de TI.

Os sistemas e computadores devem ter versões de *software* antivírus instalados, ativados e atualizados permanentemente. Em caso de suspeita de incidência de vírus ou problemas de funcionalidade de *hardware* ou *software*, o colaborador deverá acionar o suporte de TI da Inovar Previdência.

É proibido executar programas, instalar equipamentos, armazenar arquivos ou promover ações que possam facilitar o acesso de usuários não autorizados à rede corporativa da Inovar Previdência.

Neste sentido, ainda é vedado ao colaborador executar programas que tenham como finalidade a decodificação de senhas, o monitoramento da rede, a leitura de dados de terceiros, a propagação de vírus de computador, a destruição parcial ou total de arquivos ou a indisponibilidade de serviços e executar programas, instalar equipamentos, armazenar arquivos ou promover ações que possam facilitar o acesso de usuários não autorizados à rede corporativa da empresa.

4.12. Arquivos nos Servidores Virtuais Externos (Nuvem)

As pastas e arquivos da Inovar Previdência são armazenados em servidores virtuais externos (nuvem) e devem ser obrigatoriamente utilizadas, evitando a permanência de arquivos para execução das tarefas em HD local sem função de *backup* diário.

As Informações restritas e confidenciais, bem como os Dados Pessoais são restritos aos colaboradores que necessitam conhecê-los para desenvolvimento de suas atividades, sendo o controle de acesso feito pelo próprio serviço de armazenamento.

Não é permitido ao colaborador a armazenagem na nuvem de arquivos que não guardem relação com as atividades desenvolvidas pela Inovar Previdência ou que firam quaisquer princípios estabelecidos nesta Política.

O colaborador é responsável pelas atividades realizadas por intermédio de sua conta de usuário e senhas de acesso no acesso aos arquivos armazenados em nuvem, não podendo fornecer e/ou compartilhar seu usuário, senha e/ou acesso à rede com outros usuários.

4.13. Utilização de Sistemas Externos

Os Sistemas Externos são utilizados para gestão das atividades da Inovar Previdência, de ordem operacional, financeira e para cumprimento de obrigações legais ou regulatórias. Cada colaborador possui o seu *login* e senha para acesso a estes sistemas.

É expressamente proibida a divulgação e/ou o compartilhamento indevido das Informações e/ou Dados Pessoais contidos nos sistemas externos, devendo todos os colaboradores fazer uso dessas aplicações em estrito interesse da Inovar Previdência, mantendo conduta profissional.

4.14. Utilização da Internet

Sob o aspecto de proteção e integridade dos sistemas de informação, a Internet é classificada como conexão de alto risco.

As regras contidas nesta Política visam também o desenvolvimento de um comportamento ético e profissional do uso da Internet. Os colaboradores devem estar cientes, portanto, das peculiaridades da navegação na Internet, antes de acessá-la e de utilizar os seus recursos.

A Internet, via cabo ou *Wi-fi*, deverá ser utilizada para fins profissionais, como ferramenta de busca de informações, que contribuam para o desenvolvimento das atividades da Inovar Previdência.

O colaborador é responsável pelas atividades realizadas por intermédio de sua conta de usuário e senhas de acesso.

Em particular, o usuário deverá observar os termos de licença de uso do material obtido através da Internet.

Como é do interesse da Inovar Previdência que seus colaboradores estejam bem informados, o uso de sites de notícias ou de serviços, por exemplo, é aceitável, desde que não comprometa a banda da rede em horários estritamente comerciais, não perturbe o bom andamento dos trabalhos.

Os colaboradores da Inovar Previdência não deverão:

a) Utilizar a Internet com objetivos ou meios para a prática de atos ilícitos, proibidos pela lei ou pela presente Política, lesivos aos direitos e interesses da Entidade ou de terceiros;

b) Utilizar a Internet com objetivo de danificar, inutilizar, sobrecarregar ou deteriorar os recursos de tecnologia da informação e dados de qualquer tipo, de uso corporativo, pessoal ou de terceiros;

c) Acessar a sites de *proxy* com o objetivo de burlar os mecanismos de segurança existentes;

d) Acessar sites de pornografia, pedofilia e outros contrários à lei. O acesso a esses sites é terminantemente proibido, ainda que os mesmos não estejam bloqueados no sistema de segurança da Instituição.

Os equipamentos fornecidos para o acesso à Internet são de propriedade da Inovar Previdência que poderá analisar e, se necessário, bloquear qualquer arquivo, site, e-mail, domínio ou aplicação armazenados na rede ou Internet, estejam eles em disco local ou na rede. Assim, a Entidade, em total conformidade legal, reserva-se o direito de monitorar e registrar todos os acessos de seus colaboradores à rede de Internet.

Em caso de *home office*, os colaboradores deverão utilizar sua rede doméstica para acesso à Internet, permanecendo as mesmas obrigações constantes desta Política.

4.15. Utilização de e-mail (Correio Eletrônico)

Os serviços de correio eletrônico são oferecidos como um recurso profissional pela Inovar Previdência para seus colaboradores no cumprimento de seus objetivos nas áreas de atuação. Cada colaborador é responsável por utilizar os serviços de correio eletrônico de maneira profissional, ética e legal. Deve ser considerado que o correio eletrônico é inerentemente uma forma insegura de comunicação, não garantindo sigilo ou entrega.

O uso pessoal poderá ser permitido, mas não priorizado, desde que não provoque efeitos negativos para qualquer outro usuário, não viole o sistema de mensagens, não interfira nas suas atividades, não interfira direta ou indiretamente nas operações dos recursos computacionais e serviços de correio eletrônico da Entidade, não incorra em gastos adicionais ou viole qualquer outra lei ou norma vigente.

O acesso às mensagens nos servidores de correio eletrônico deve ser feito usando protocolos seguros. Os colaboradores com acesso aos serviços de mensagem eletrônica disponibilizados pela Inovar Previdência devem observar o seguinte:

a) Todos os usuários dos ativos de informação de propriedade da Inovar Previdência, ao utilizarem esse serviço, deverão fazê-lo no estrito interesse da Entidade, mantendo uma conduta ética e profissional;

b) Todas as contas de e-mail terão uma titularidade, sendo o usuário titular o responsável direto pelas mensagens enviadas por intermédio do seu endereço de e-mail;

c) Os usuários poderão ser titulares de uma única caixa postal individual no servidor de e-mail, com direitos de envio/recebimento de mensagens, via Intranet e Internet, bem como serem receptores das mensagens encaminhadas para os e-mails de comunicação da Entidade;

d) Contas com inatividade por um período igual ou superior a 60 (sessenta) dias, sem motivo justificado, a exemplo dos afastamentos ou licenças, poderão ser bloqueadas, a fim de evitar o recebimento de novas mensagens;

e) O usuário deve utilizar o e-mail de forma adequada e diligente;

f) É vedado o envio, armazenamento ou manuseio de material que caracterize a divulgação, incentivo ou prática de atos que:

- Contrariem o disposto na legislação vigente, ética, moral e de ordem pública;
- Sejam proibidos pela presente Política, lesivos aos direitos e interesses da Inovar Previdência ou de terceiros;
- De qualquer forma, possam danificar, inutilizar, invadir, sobrecarregar ou deteriorar os recursos tecnológicos (*hardware* e *software*), bem como os documentos e arquivos de qualquer tipo, do usuário ou de terceiros;
- Promovam ameaças, difamação ou assédio a outras pessoas;
- Contenham conteúdo considerado impróprio, obsceno ou ilegal;
- Sejam de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico entre outros;
- Contenham a prática de qualquer tipo de discriminação relativa a raça, sexo, credo religioso, incapacidade física ou mental ou outras situações protegidas; e
- Caracterizem violação de direito autoral garantido por lei.

g) É vedada ainda a utilização do e-mail, nas situações abaixo:

- Acesso não autorizado à caixa postal de outro usuário;
- Uso para atividades com fins comerciais ou políticos e o uso extensivo para assuntos pessoais ou privados;
- Envio de mensagens do tipo "corrente" e "*spam*";
- Envio intencional de mensagens que contenham vírus eletrônico ou qualquer forma de rotinas de programação de computador, prejudiciais ou danosas;
- Utilização de listas e/ou caderno de endereços da Inovar Previdência para a distribuição de mensagens que não sejam de estrito interesse funcional e sem a devida permissão do responsável pelas listas e/ou caderno de endereços em questão;
- Divulgação de informações em não conformidade com a diretriz de Classificação de Informações prevista nesta política;
- Envio de qualquer mensagem que torne a Entidade vulnerável a ações civis ou criminais; e
- Exclusão de mensagens relacionadas às atividades profissionais, quando a Entidade ou pessoas a ele relacionadas estiverem sujeitos a algum tipo de investigação.

Os usuários devem utilizar em sua assinatura padrão texto que identifica os requisitos de Segurança da Informação relacionados a confidencialidade da troca de informações, servindo como instrução a terceiros que recebam mensagens provenientes da Inovar Previdência:

> *"Esta mensagem, inclusive seus anexos, pode conter informações confidenciais e dados pessoais, de uso restrito e legalmente protegidos. Caso você tenha recebido esta mensagem indevidamente, por gentileza, exclua-a de seus sistemas e comunique imediatamente o remetente. É proibida qualquer forma de tratamento do conteúdo desta mensagem ou de parte dela, incluindo utilização, reprodução e/ou divulgação sem autorização expressa de seu remetente e em desacordo com a legislação vigente, em especial, a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais)".*

4.16. Utilização de *software* de Mensagens Instantâneas e Redes Sociais

Os serviços de comunicação instantânea instalados nos equipamentos serão inicialmente disponibilizados aos colaboradores que necessitem dessa ferramenta e poderão ser bloqueados, caso o gestor requisite formalmente ao suporte de TI da Entidade.

O uso de aplicativos de comunicação pelos colaboradores, a partir de recursos da Inovar Previdência, para compartilhar informações profissionais, deverá ser feito de forma responsável para evitar riscos desnecessários, que possam comprometer as atividades, os projetos, as Informações e Dados Pessoais ou a própria Entidade.

O colaborador deve, ainda, preservar o sigilo e a confidencialidade das Informações e Dados Pessoais, atender aos requisitos de segurança previstos nesta Política e respeitar a legislação vigente durante o uso de serviços de comunicação instantânea.

4.17. Utilização de Dispositivos Móveis Corporativos

Dispositivos móveis corporativos são equipamentos portáteis dotados de capacidade computacional, entre os quais se incluem, não se limitando a estes: *notebooks*, *netbooks*, *smartphones* e *tablets*.

O colaborador deve utilizar os dispositivos móveis corporativos de forma adequada e diligente, de forma a prevenir ações que possam danificar, inutilizar, sobrecarregar ou deteriorar os recursos tecnológicos (*hardware* e *software*), bem como os documentos e arquivos de qualquer tipo, de seu uso ou de uso de terceiros.

O usuário é pessoalmente responsável por todas as atividades realizadas por intermédio de dispositivos móveis corporativo, tanto por sua guarda quanto pelos conteúdos neles instalados.

É responsabilidade do colaborador, no caso de furto ou roubo de um dispositivo móvel fornecido pela Inovar Previdência, notificar imediatamente seu gestor e o suporte de TI. Também deverá, assim que possível, registrar um Boletim de Ocorrência no Distrito Policial (B.O.).

O colaborador deverá estar ciente de que o uso indevido do dispositivo móvel caracterizará a assunção de todos os riscos da sua má utilização, sendo o único responsável por quaisquer danos, diretos ou indiretos, presentes ou futuros, que venha causar à Entidade e/ou a terceiros.

Em caso de desligamento, o colaborador deve realizar imediata devolução, não realizando formatação, instalação ou desinstalação de *softwares* e aplicações, alterações de senhas ou quaisquer outras ações semelhantes sem o devido conhecimento do terceiro responsável por TI, de seus dispositivos móveis ao Recursos Humanos da Entidade ou ao gestor responsável.

Constituem boas práticas de segurança para dispositivos móveis:

a) Quando em deslocamentos de carro, coloque o *notebook* no porta-malas ou em local não visível;

b) Ao movimentar-se com o *notebook*, se possível, não utilize malas convencionais para *notebook* e sim mochilas ou malas discretas;

c) Não coloque o *notebook* em carrinhos de aeroportos, nem despache junto à bagagem;

d) Em locais públicos (recepção de hotéis, restaurantes e aeroportos dentre outros), mantenha o *notebook* próximo e sempre à vista, não se distanciando do equipamento;

e) Evite utilizar o *notebook* em locais públicos;

f) Nos hotéis e outras hospedagens, sempre que possível, guarde o *notebook* no cofre do seu apartamento;

g) Avalie se em pequenas viagens, o dispositivo móvel corporativo é necessário;

h) Utilize bloqueio de tela com senha;

i) Se possível utilize a opção de criptografia para cartões SD utilizados em tablets e celulares; e

j) Não conecte em redes *Wi-Fi* desconhecidas: essas redes podem conter mecanismos para captura de dados do seu dispositivo.

4.18. Utilização de Mídias Removíveis

Dispositivos removíveis possuem memória para armazenamento, incluindo mas não se limitando a *pen drives*, USB *drives*, HD externos e cartões de memória.

O uso de mídias removíveis deve ser tratado como exceção à regra, pois a porta USB é o principal ponto de vulnerabilidade de segurança, podendo ser usada para a fuga de Informações e Dados Pessoais.

Os usuários de mídias removíveis são diretamente responsáveis pelos riscos e impactos que tais dispositivos possam vir a causar, tendo em vista a possibilidade desse tipo de mídia conter vírus e *softwares* maliciosos, capazes de danificar e corromper dados e dispositivos.

Caso seja necessário transportar arquivos através de mídias removíveis (HD externo ou *pen drive*) é recomendado que os arquivos sejam criptografados e apagados, posteriormente, afim de evitar vazamento de Informações e/ou Dados Pessoais.

4.19. Comunicação Verbal dentro e fora da Entidade

Somente os colaboradores que estão devidamente autorizados a falar em nome da Inovar Previdência, para os meios de comunicação, podem fazê-lo em nome da Entidade.

A fim de evitar exposição desnecessária da Inovar Previdência, os colaboradores não devem tratar de assuntos internos e confidenciais em locais públicos ou dentro das instalações físicas da Entidade, quando próximos a visitantes ou terceiros.

4.20. Engenharia Social

É um termo utilizado coloquialmente que representa a habilidade de enganar pessoas com o objetivo de obter Informações e/ou Dados Pessoais.

Essa ação pode ocorrer de diversas formas, mas o comum é os engenheiros utilizarem a falta de conscientização dos colaboradores em relação à Segurança da Informação da Entidade. O ataque pode ser feito (i) de forma direta, quando há um contato entre o engenheiro social e a vítima, por meio de telefonemas ou pessoalmente, ou (ii) de forma indireta, quando há a utilização de *softwares* ou outras ferramentas, a fim de captar dados que facilitem o acesso às informações desejadas. Podem ser, por exemplo, mensagens que contenham avisos de premiações, ofertas de sociedade em grandes somas de dinheiro, heranças e negócios em outros países etc.

Assim, caso o colaborador, ainda que a tentativa de ataque tenha ocorrido por outros meios (não tecnológicos), tenha conhecimento de qualquer forma de Engenharia Social, deverá comunicar ao gestor responsável e ao suporte de TI.

5. RESPONSABILIDADES

A correta utilização dos recursos disponibilizados é dever de todos os colaboradores da Entidade, sendo que o uso indevido, negligente ou imprudente será responsabilizado, conforme normativos internos e legais.

A Inovar Previdência reserva-se o direito de analisar dados e evidências, a fim de obter provas que possam ser utilizadas nos processos investigatórios, bem como, de adotar as medidas legais cabíveis.

Quanto à presente Política da Inovar Previdência, as responsabilidades ficam assim distribuídas:

5.1. Conselho Deliberativo

a) Aprovar a Política de Segurança da Informação; e

b) Determinar a adoção de medidas necessárias para seu cumprimento.

5.2. Diretorias e Gestores

a) Implantar e fazer cumprir as normas presentes nesta Política;

b) Assegurar que as equipes possuam acesso e conhecimento desta Política, orientando e informando os colaboradores sobre as práticas necessárias à Segurança da Informação;

c) Apoiar, incentivar e acompanhar a participação ativa de todos subordinados no Plano de Divulgação e Treinamento, definido pelas áreas de *compliance*, comunicação e Recursos Humanos;

d) Promover, conjuntamente com o suporte de TI, a segregação de acessos às Informações e Dados Pessoais nos sistemas da Inovar Previdência, evitando conflitos de interesse e adotando perfis de acesso.

e) Receber o reporte de todo e qualquer usuário e/ou área para tratar de assuntos pertinentes à Segurança da Informação de que trata este instrumento; e

f) Receber e tratar as notificações dos casos de violação das diretrizes de segurança expostas neste instrumento.

5.3. Suporte de TI

Sempre que requerido pela Inovar Previdência:

a) Configurar os equipamentos, instalar *softwares* e implementar os controles necessários, bem como definir regras para a instalação de *software* e *hardware* nos equipamentos da Entidade;

b) Executar as ações necessárias para tratar violações de segurança no âmbito tecnológico;

c) Promover a recuperação de sistemas e aparelhos, se necessário;

Com periodicidade de seis meses a no máximo, um ano:

d) Monitorar o ambiente de TI e a atividade de todos os usuários durante os acessos às redes internas e externas (Internet), por exemplo: sites, e-mails, sistemas e outros;

e) Administrar, proteger e testar cópias de segurança de sistemas e dados relacionados aos processos operacionais considerados críticos;

f) Planejar e monitorar a capacidade de armazenagem, processamento e transmissão necessários para garantir a segurança requerida e a disponibilidade da rede interna;

g) Assegurar-se de que não sejam introduzidas vulnerabilidades ou fragilidades na rede e nos equipamentos;

h) Coordenar as atividades de tratamento e resposta a incidentes de TI;

i) Promover e rever juntamente com os gestores a segregação de acessos necessários aos sistemas da Inovar Previdência, evitando conflitos de interesse e adotando perfis de acesso;

j) Promover e rever guarda de *logs* de auditoria dos sistemas da Inovar Previdência, sempre que os mesmos forne-cerem a referida possibilidade; e

k) Realizar testes e atualizações nos diversos acessos aos recursos de TI.

5.4. Área de Controles Internos/*Compliance*

a) Avaliar os riscos do processo juntamente com os responsáveis;

b) Elaborar e executar planos de testes e realizar auditoria nos controles relacionados à Segurança da Informação; e

c) Monitorar o resultado e sugerir novos controles no ambiente de Segurança da Informação, quando aplicável.

5.5. Todos os colaboradores da Inovar Previdência

a) Conhecer e cumprir a presente Política;

b) Assinar Termo de Ciência e Responsabilidade sobre a Política declarando ter conhecimento de suas responsabilidades;

c) Buscar orientação em caso de dúvidas relacionadas à Segurança da Informação;

d) Fiscalizar e orientar os prestadores de serviços da Entidade quanto às diretrizes desta Política;

e) Observar os princípios constantes do Estatuto Social, Código de Ética da Entidade e Política de Privacidade da Inovar Previdência; e

f) Comunicar imediatamente quando do descumprimento ou violação desta Política.

6. DIVULGAÇÃO E TREINAMENTO

Os gestores, as áreas de Controles Internos/*Compliance* e de Comunicação deverão definir um Plano de Divulgação e Treinamento a fim de que todos os colaboradores estejam cientes das normas constantes nesta Política.

Os colaboradores atuais e aqueles futuramente contratados deverão assinar Termo de Responsabilidade e Confidencialidade, comprometendo-se a agir conforme as diretrizes aqui estipuladas.

7. TRATAMENTO DE VIOLAÇÕES e RESPONSABILIDADES

Todas violações a esta Política serão investigadas para a determinação das medidas necessárias, visando à correção da falha ou reestruturação de processos. Situações que podem ocasionar sanções incluem, mas não se limitam, a:

a) Uso ilegal de *software*;

b) Introdução (intencional ou não) de vírus de informática;

c) Tentativas de acesso não autorizado a dados e sistemas; e/ou

d) Compartilhamento de Informações e Dados Pessoais de maneira contrária à legislação e/ou às determinações desta Política.

Ainda, a fim de garantir a confidencialidade, integridade e disponibilidade das Informações e Dados Pessoais, ao tomar conhecimento de todo e qualquer incidente de Segurança da Informação que ocorrer em ambiente próprio ou de terceiros, de sua responsabilidade, e que possa comprometer as atividades da Inovar Previdência, especialmente acessos não autorizados e situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma inadequada ou ilícita, o colaborador deverá notificar o gestor responsável e o suporte de TI.

Caso devidamente comprovado, o usuário infrator estará passível das seguintes penalidades imediatas, sem prévio aviso:

a) Descredenciamento da senha de acesso à Internet;

b) Cancelamento da conta de e-mail;

c) Cancelamento do acesso aos sistemas corporativos;

d) Desativação do ponto de rede do usuário;

e) Aplicação das penalidades previstas na legislação vigente no Brasil.

Nas mesmas penas incorrem o colaborador que, ciente do incidente com as Informações e Dados Pessoais, deixa de comunicar o gestor e/ou suporte de TI.

O colaborador, caso devidamente constatado que agiu com dolo ou culpa, no compartilhamento de Informações e/ou Dados Pessoais, se responsabilizará pelo pagamento de valores, importâncias ou quantias que o incidente e/ou tratamento inadequado tenha causado à Inovar Previdência que incluem: (i) indenizações do dano causado à Entidade; (ii) multas e penalidades impostas à Inovar Previdência; e (ii) custos de defesa, caso necessário que a Entidade se defenda judicialmente em decorrência do vazamento de Informações e/ou Dados Pessoais.

8. GESTÃO DE CONTINUIDADE DE NEGÓCIOS

A Gestão de Continuidade de Negócios define os procedimentos para prevenção de interrupções de atividades críticas ao negócio, viabilizando a ativação de processos alternativos na ocorrência de indisponibilidade dos serviços. Também visa orientar os colaboradores em relação aos procedimentos a serem realizados quando da ocorrência de algum incidente, informando as partes interessadas.

A gestão de continuidade de negócios é um processo permanente destinado a preparar a Inovar Previdência a resistir aos efeitos de emergências ou interrupções e minimizar os danos operacionais, legais, financeiros e à imagem da Entidade.

As emergências e interrupções podem ser as mais variadas, mas inevitavelmente resultarão em três cenários: indisponibilidade de acesso físico ao local de trabalho (ex.: incêndio, desabamento), indisponibilidade de pessoas-chave (ex.: afastamento em massa), e indisponibilidade de TI (ex.: queda do link, dano ao datacenter).

Desta forma, a gestão de continuidade de negócios prepara os passos a serem tomados após uma emergência ou interrupção para a retomada das atividades críticas e posterior retorno à normalidade.

A Inovar Previdência, para conseguir atingir tal objetivo implantará as seguintes etapas:

- **Conhecer a unidade:** nessa etapa denominada "análise de impacto nos negócios", os gestores e suporte de TI da Inovar Previdência, na unidade de trabalho, irá identificar:
  a) suas atividades críticas;
  b) o tempo máximo que tais atividades podem ficar paradas sem que acarretem um dano insuportável à Inovar Previdência;
  c) os danos decorrentes da paralização;
  d) a identificação das pessoas responsáveis pelas atividades críticas, bem como as capacitadas a realizá-las;
  e) os sistemas utilizados na execução das atividades críticas;
  f) os dados vitais requeridos nas atividades críticas, bem como informações de cópia de segurança;
  g) os recursos mínimos necessários à execução das atividades críticas;
  h) os riscos de acontecer um cenário de indisponibilidade de acesso físico, de indisponibilidade de TI e de indisponibilidade de pessoas; e
  i) possíveis locais alternativos de trabalho.

Após identificação, será elaborado Relatório de Impacto aos Negócios, documento que servirá de base para as próximas etapas.

- **Definição de estratégias:** nessa fase são utilizadas informações colhidas durante o conhecimento da unidade para identificar e escolher opções de estratégias de continuidade.

A estratégia de continuidade habilita a unidade a continuar suas atividades críticas dentro do período máximo em que ela pode ser interrompida, antes que danos insuportáveis advindos da interrupção ocorram.

São definidas estratégias para:

1. **Local de trabalho:** definição de local alternativo no caso de indisponibilidade de acesso, bem como procedimentos a serem adotados;
2. **Pessoas:** disseminação de conhecimentos, mapeamento de processos, alocação de trabalhos na indisponibilidade de pessoas;
3. **Tecnologia da Informação:** procedimentos a serem realizados no caso de indisponibilidade dos recursos de TI e métodos de mitigá-la.

- **Elaboração e implementação de um ou mais planos:** após a seleção dos processos críticos e a definição das estratégias, serão elaborados um ou mais planos que possibilitem a implementação dessas estratégias.
- **Testes:** a gestão de continuidade de negócio e seus planos serão testados, auditados e mantidos por meio de revisões e atualizações periódicas constantes pela Inovar Previdência.

9. VIGÊNCIA, VALIDADE E ATUALIZAÇÕES

A presente Política passa a vigorar a partir da data de sua aprovação pelo Conselho Deliberativo, sendo válida por tempo indeterminado.

Após a implantação desta Política, com o objetivo de mantê-la atualizada e condizente com as necessidades da Entidade, deverão ser realizadas, anualmente, ou sempre que houver incidentes, revisões com a implantação de novas ações e controles para sua melhoria continua.

10. REFERÊNCIAS

a) ABNT NBR ISO/IEC 27001:2013 Tecnologia da informação – Técnicas de segurança – Sistemas de Gestão da Segurança da Informação – Requisitos;

b) ABNT NBR ISO/IEC 27002:2013 Tecnologia da informação – Técnicas de segurança – Código de prática para controles de segurança da informação;

c) Constituição da República Federativa do Brasil de 1988;

d) Lei 9.609/98 – Lei do *Software*;

e) Lei 12.965/14 – Marco Civil da Internet; e

f) Lei 13.709/18 – Lei Geral de Proteção de Dados Pessoais.

11. GLOSSÁRIO

Ambiente Tecnológico
Compreende todos os sistemas, computadores e redes da Entidade.

Antivírus
Programa de proteção do computador que detecta e elimina os vírus (programas danosos) nele existentes, assim como impede sua instalação e propagação.

Aplicativos de comunicação
Programas de computador, geralmente instalados em dispositivos móveis, usados para troca rápida de mensagens, conteúdos e informações multimídia, a exemplo de *Whatsapp*, *Telegram*, *Skype* etc.

Ativo
Qualquer coisa que tenha valor para a Entidade e precisa ser adequadamente protegida.

Backup
É a cópia de dados de um dispositivo de armazenamento a outro para que possa ser restaurado em caso da perda dos dados originais, o que pode envolver apagamentos acidentais ou corrupção de dados.

Colaboradores
Colaboradores da Inovar Previdência, incluindo os membros da Diretoria e dos Conselhos Deliberativo e Fiscal.

Dados Pessoais
Informação relacionada a pessoa natural identificada ou identificável.

Dados Pessoais Sensíveis
Dado Pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

Dispositivos móveis
Equipamentos de pequena dimensão que têm como características a capacidade de registro, armazenamento ou processamento de informações, possibilidade de estabelecer conexões e interagir com outros sistemas ou redes. Exemplos: *smartphone*, *notebook*, *tablet*, câmeras de fotografia ou filmagem.

Hardware
conjunto dos componentes físicos (material eletrônico, placas, monitor, equipamentos periféricos etc.) de um computador.

Informação
Conjunto de dados e conhecimentos organizados, que possam constituir referências sobre um determinado acontecimento, fato ou fenômeno.

Log
Registro de eventos em um sistema de computadores.

Mídias Removíveis
Dispositivos que permitem a leitura e gravação de dados tais como CD, DVD, Disquete, *Pen Drive*, cartão de memória entre outros.

Prestadores de Serviços
Pessoas Físicas ou Jurídicas que possuem relação de negócios com a Entidade.

Perfil de Acesso
Grupo de acessos a um recurso tecnológico estratificado por função dentro da Entidade.

Servidor
é um *software* ou computador, com sistema de computação centralizada que fornece serviços a uma rede de computadores, chamada de cliente.

Software
É a parte lógica, o conjunto de instruções e dados processados nos servidores e computadores.

Spam
Mensagem de e-mail publicada em massa com fins publicitários.

TI
Tecnologia da Informação.

USB
É um tipo de conexão "ligar e usar" que permite a conexão de periféricos sem a necessidade de desligar o computador.

Wi-Fi
Abreviação de *Wireless Fidelity* – é uma tecnologia de comunicação que não faz uso de cabos e, geralmente, é transmitida através de frequências de rádio, infravermelhos etc.

INOVAR PREVIDÊNCIA – SOCIEDADE DE PREVIDÊNCIA PRIVADA

Rua Correia Dias, 184 - 7º Andar - Conj. 71 - Paraíso, SP - CEP 04104-000

(11) 4210-2420 contato@inovarprevidencia.com.br www.inovarprevidencia.com.br www.inovarprevidencia.com.br/familia