BIBLIOTECA DE POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE DE DADOS PESSOAIS PARA FORNECEDORES

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA PREVCOM.

1. Sumário

2. POLÍTICA SEGURANÇA DA INFORMAÇÃO CORPORATIVA

2.1. OBJETIVO

Definir as diretrizes para a implantação de práticas voltadas para a Segurança da Informação com a implementação de classificação, controles e gestão da informação. O objetivo é preservar a confidencialidade, integridade, disponibilidade e autenticidade da informação em todos os ambientes, buscando a proteção dos dados críticos da Fundação de Previdência Complementar do Estado de São Paulo, que compreende doravante a marca PREVCOM, e de sua reputação no mercado, mitigando eventuais prejuízos financeiros.

Também é importante mencionar que a PREVCOM tem como uma de suas premissas a proteção dos dados pessoais de todas as pessoas envolvidas na sua cadeia de atividades. O direito à privacidade é uma prioridade e pauta todas as ações e políticas da PREVCOM. Dentre as atividades abrangidas por esta política, poderá ocorrer o Tratamento de dados pessoais, ou seja, operações realizadas com dados pessoais, tais como, a coleta, produção, utilização, acesso, distribuição, processamento, arquivamento, eliminação, entre outros. Desta forma, qualquer Tratamento de dados realizado deverá respeitar as disposições gerais desta Política além dos demais documentos corporativos e políticas aplicáveis ao tema.

2.2. APLICAÇÃO

Aplica-se a todo e qualquer usuário com acesso a qualquer tipo de informação da Fundação de Previdência Complementar do Estado de São Paulo, independente do seu vínculo com a Fundação, seja ele gestor, colaborador, estagiário, temporário, terceiro ou de qualquer forma no âmbito de representante e/ou parceiro de negócios. Também se aplica a qualquer ativo de informação, seja nos servidores, sistemas, *desktops*, *notebooks*, *smartphones*, *tablets* ou a qualquer dispositivo de armazenamento, processamento ou tráfego de informações.

2.3. PRINCÍPIOS GERAIS

Os princípios estabelecidos nesta política visam permear os tópicos que apresentam relacionamento direto ou indireto com aspectos de segurança das informações, classificação, controle e gestão dessas informações utilizadas e/ou geradas da Fundação de Previdência Complementar do Estado de São Paulo (PREVCOM) em seu desempenho corporativo.

Esses princípios devem ser desdobrados em diretrizes e instruções, por meio de diferentes normativos visando à sua correta aplicação, execução, controle e monitoramento.

As diretrizes devem expressar estratégias, valores e o nível de comprometimento que a PREVCOM estabelece em relação à Segurança da Informação Corporativa, bem como as respectivas instruções devem orientar o quadro de colaboradores quanto ao cumprimento de atividades e rotinas relacionadas ao tema.

Todos os esforços de segurança da informação devem ser projetados, implantados e mantidos buscando suportar os requisitos de negócio da PREVCOM, observando práticas de análise de risco e procurando um alinhamento a esta política.

Situações específicas não contempladas ou que estejam conflitantes com esta política devem ser analisadas pela equipe de TI, formalizadas por meio de documento próprio e apresentadas à Diretoria Executiva e a Comissão Consultiva de Mudanças Segurança e Privacidade da PREVCOM para a aprovação e continuidade do processo. As áreas de Risco, Controles Internos ou Auditoria poderão ser envolvidas sempre que se fizer necessário.

A revisão desta política e dos normativos derivados devem ser realizados de forma periódica para que esses instrumentos estejam permanentemente atualizados.

A PREVCOM reserva-se o direito de, a qualquer momento e sem aviso prévio, monitorar, auditar ou fazer cópias de segurança de qualquer dado e/ou informação armazenado (s) em ativos de sua propriedade.

2.4. ATIVOS DE INFORMAÇÃO

Os ativos de informação vinculados à Fundação pertencem a PREVCOM, não importando seu meio físico ou lógico de armazenamento. Seu uso se dará apenas e tão somente dentro do escopo das atividades de negócio da PREVCOM.

Controles tecnológicos e/ou processuais serão utilizados com o objetivo de proteger e minimizar os riscos associados ao uso das informações ou ativos de processamento de modo a preservar suas características de segurança.

A gestão de ativos da informação deve especificar, sempre que possível, requisitos para inventariar e identificar o responsável dos ativos de informação, independente do seu meio de acesso, mantendo a proteção adequada de acordo com a proteção ideal.

A informação produzida ou transformada por qualquer processo da PREVCOM é considerada como um ativo da Fundação. Desta forma, os ativos de informação da PREVCOM, assim como os seus respectivos ativos de processamento, devem ser identificados, controlados e armazenados adequadamente de forma a proteger seus requisitos de integridade, confidencialidade, legalidade e disponibilidade.

Todas as pessoas físicas ou jurídicas que prestam serviços internos ou externos devem utilizar os ativos de acordo com as cláusulas contratuais firmadas com fornecedores, parceiros e clientes. A utilização de ativos da informação deve respeitar a legislação vigente e as normas e políticas internas da PREVCOM.

2.5. ORGANIZAÇÃO DA SEGURANÇA DA INFORMAÇÃO

Todos os assuntos que tenham relacionamento com a TI - Tecnologia da Informação da PREVCOM deverão ser analisados e tratados dentro da esfera adequada, seguindo os princípios e definições desta política.

Para a aplicação e o acompanhamento dos tópicos relativos à Segurança da Informação Corporativa, fica estabelecido o endereçamento a Comissão Consultiva de Mudanças Segurança e Privacidade e suas subcomissões.

Devem ser estabelecidos canais de comunicação específicos, possibilitando os meios necessários à realização de denúncias de não aderência aos princípios desta política ou outras situações que ponham em risco a segurança das informações da PREVCOM.

2.6. CLASSIFICAÇÃO DOS ATIVOS DA INFORMAÇÃO

Os ativos de informação deverão ser classificados de acordo com seu nível de confidencialidade, disponibilidade, integridade e características legais de controle, de forma a serem adequadamente protegidos, acessados, armazenados, tratados, transportados e descartados, conforme apresentado abaixo:

- **ESTRITAMENTE CONFIDENCIAL:** Esta categoria se aplica à informação que deve ser utilizada somente dentro do âmbito da PREVCOM, restrita a um grupo limitado de componentes. Sua divulgação não autorizada pode impactar muito seriamente a PREVCOM e seus clientes.
- **USO INTERNO:** Esta categoria se aplica à informação que se destina ao uso dentro do âmbito da PREVCOM.
- **PÚBLICA:** Esta categoria se aplica à informação que pode ser divulgada e acessada pelo público em geral e para a qual sua divulgação e conhecimento generalizado não causam nenhum conflito ou dano, nem a PREVCOM e nem a terceiros.

Todos os ativos de informações, quando não estiverem devidamente classificados, identificados ou divulgados devem ser considerados de uso interno.

2.7. SEGURANÇA FÍSICA E DO AMBIENTE

Os ativos de informação devem ser protegidos contra danos (acidentais ou intencionais), roubo e/ou interrupções ou quaisquer eventos que gerem sua indisponibilidade.

Deve ser estabelecido um perímetro mínimo de segurança física de forma a preservar o acesso somente a pessoas devidamente autorizadas para tal, conforme previsto normativo sobre o tema.

A prática de mesa limpa deverá ser adotada, de forma a promover a segurança dos ativos de informação, classificados como estritamente confidenciais, bem como o processamento e a guarda de dados críticos devem ser efetuados em áreas com segurança apropriada.

2.8. SEGURANÇA DE RECURSOS HUMANOS

O processo de recrutamento e seleção de candidatos, cujos critérios estão descritos em normativo específico, deve apresentar aos aprovados os princípios da PREVCOM e de conduta relacionados nas Políticas de Governança Corporativa e Código de Ética.

Toda quebra das regras de confidencialidade pelo quadro de colaboradores, bem como qualquer ação que venha a violar os termos desta política deverá ser tratada pelo Comitê de Ética.

Os acordos de confidencialidade de informações devem ser incluídos nos termos dos contratos de trabalho ou prestação de serviço, os quais devem ser assinados pelos envolvidos ou seus responsáveis legais. As responsabilidades dos colaboradores devem ser estabelecidas no que concerne à segurança dos ativos de informação sob sua tutela.

Cláusulas apropriadas que regem a segurança, a privacidade dos dados, os requisitos regulatórios, a Propriedade Intelectual e a confidencialidade devem ser incluídas em todos os contratos para salvaguardar os interesses da PREVCOM.

A utilização de terceirizados e/ou prestadores de serviços em processos nos quais informações “estritamente confidenciais” ou “internas” sejam trabalhadas, devem ser particularmente controladas por meios cabíveis (contratos e processos de monitoração), de forma a contemplar os requisitos de segurança da informação estabelecidos pela PREVCOM.

Todo novo parceiro contratado pela PREVCOM deve atender aos requisitos de TI - Tecnologia da Informação previstos em normativo específico sobre o tema.

Todo colaborador da PREVCOM, quando for desligado, deverá entregar os recursos que lhe foram disponibilizados pela Fundação *(notebooks*, *smartphones*, etc.).

Os direitos de acesso de todos os usuários de tecnologia devem ser removidos após a rescisão de seu contrato ou ajustados após a alteração. O acesso aos ativos de informações deve ser revogado a partir da data de término ou rescisão do respectivo contrato.

2.9. TRATAMENTO DE FRAUDE

Controles específicos que visem à redução das possibilidades de fraude devem ser implementados de forma sistêmica, tais como:

- Validação periódica dos acessos quanto à sua necessidade e aderência funcional;
- Segregação de funções entre os usuários;

- Funcionalidades relacionadas a rastreabilidade das ações nos sistemas;

Todas as ocorrências de fraudes devem ser **investigadas**, **registradas** e **tratadas** de forma condizente com a dimensão da situação pelas áreas responsáveis pela sua prevenção.

2.10. UTILIZAÇÃO DE CORREIO ELETRÔNICO, TELEFONIA E INTERNET

Os serviços de acesso à internet, correio eletrônico e telefonia fixa também são ativos da PREVCOM disponibilizados para a realização das atividades durante a jornada de trabalho. Desta forma, os usuários não devem utilizar os recursos para fins não condizentes com suas funções e responsabilidades profissionais.

O acesso à ferramenta de Webmail da PREVCOM somente deve ser liberado mediante aprovação da área responsável, tendo em vista que este tipo de acesso é restrito a um grupo específico de pessoas.

Esses serviços corporativos não são privativos. Controles de monitoramento e acompanhamento dos serviços acessados pelos usuários devem ser estabelecidos, visando o bloqueio do acesso a sites de Internet, bate-papo e facilidades de telefonia não relacionados às necessidades corporativas da PREVCOM.

Os colaboradores da PREVCOM estão proibidos de utilizar a internet de maneira que viole os acordos de privacidade de outros usuários ou infrinja legislações vigentes (leis de direitos autorais, calúnia e difamação, etc.).

Mecanismos específicos de criptografia devem ser adotados para a transmissão de informações classificadas como “estritamente confidencial”, via internet, independente do meio de comunicação ou da mídia utilizada para tal.

2.11. CONFORMIDADE E GESTÃO DE SOFTWARE

Somente devem ser utilizados *softwares* que já estejam previamente homologados pela área de TI, não sendo tolerada a utilização de *softwares* sem licença ou cópia não autorizadas, sem permissão formal da área de TI.

Toda mudança de utilização de *software, upgrades e novas versões* devem ser previamente avaliadas e aprovadas pelas áreas envolvidas em conjunto com TI, considerando-se os impactos no ambiente computacional da PREVCOM.

Uma estrutura específica de controles internos de TI deve ser estabelecida, de forma que garanta a segurança dos sistemas que suportam o atendimento aos aspectos legais.

Deve-se estabelecer uma avaliação interna (auditoria interna) e outra avaliação independente (auditoria externa) sobre a estrutura de controles de Segurança de TI visando **identificar**, **verificar**, **validar** e **emitir** um parecer sobre sua efetividade operacional.

2.12. GESTÃO DE DISPOSITIVOS DE SEGURANÇA DE TI

A gestão de dispositivos de segurança vinculados a TI deve ser tratada única e exclusivamente pelas áreas responsáveis de TI, de forma a promover a melhor solução para cada situação.

Todos os computadores (*desktops*, *notebooks*, *laptops*, servidores etc.) instalados na PREVCOM devem ser monitorados constantemente para a eliminação de vulnerabilidades de segurança identificadas e a aplicação de correções de segurança reportadas pelos fabricantes (*patches*).

Todos os recursos computacionais da PREVCOM devem estar providos de *softwares* antivírus, bem como os processos estabelecidos que garantam a atualização das vacinas.

Notebooks, laptops e dispositivos semelhantes de colaboradores que possuem cargos elegíveis para tal devem possuir mecanismos de segurança implantados, tais como **criptografia no armazenamento de dados** e mecanismos específicos.

Mecanismos específicos de controle de *e-mails* indesejados (*spam* etc.) devem ser adotados e implementados, bem como aqueles destinados à detecção de intrusos em comunicações da rede interna corporativa com o meio externo e ainda quaisquer outras soluções protetivas que se façam necessárias.

- Aplicação de Hardening / Padrões de Configuração
    - Cabe à equipe de TI - Tecnologia da Informação desenvolver e monitorar os padrões de segurança, bem como a responsabilidade em aplicar padrões de configuração para todos os componentes dos sistemas.
- Segurança na Arquitetura das Aplicações
    - A PREVCOM deve fazer uso das boas práticas de arquitetura das aplicações e a segregação em camadas de apresentação, aplicação, banco de dados com o objetivo de proporcionar a padronização de desenvolvimento e implantação de soluções.
    - Exceções ou desvios devem ser formalizados no Documento de Aceitação de Risco (DAR) e apresentados ao Comitê Executivo de Segurança da Informação Corporativa, em conjunto com a diretoria demandante para deliberação.
- Certificados Digitais
    - Toda aplicação que contenha informações da PREVCOM e esteja hospedada em ambiente externo devem suportar comunicação com protocolo seguro.
    - Todo e qualquer certificado digital em uso na PREVCOM para aplicação interna classificada como crítica deve ser emitido utilizando a autoridade certificadora homologada pela área de TI da PREVCOM.

- Desenvolvimento e Manutenção de Sistemas
    - Devem ser estabelecidas sistemáticas que venham a promover um controle satisfatório de todas as alterações e mudanças realizadas, de tal forma que os programas que estejam em produção sejam submetidos a um controle específico, identificando e registrando as modificações significativas, avaliando o impacto potencial das mudanças, obtendo as aprovações pertinentes e comunicação às partes interessadas.
    - De forma a reduzir o risco de mau uso, acidental ou deliberado dos sistemas, deve-se aplicar uma adequada segregação de funções entre os administradores do ambiente de produção e os desenvolvedores de sistemas.
    - Todas as alterações ou desenvolvimentos nos ambientes dos sistemas devem ser realizados conforme metodologias utilizadas pela Diretoria de TI, sendo padronizadas, registradas, aprovadas, testadas e documentadas, conforme normativo específico.
    - Para proteger as aplicações web da PREVCOM e para mitigar os riscos de apropriação das vulnerabilidades, devem ser adotadas as boas práticas de desenvolvimento seguro como, por exemplo, OWASP.

2.13. CONTINUIDADE DO NEGÓCIO (BACKUP E PLANOS DE CONTINGÊNCIA)

De forma a promover a continuidade do negócio, evitando sua interrupção e a proteção dos processos críticos contra falhas ou desastres significativos devem ser estabelecidas sistemáticas que promovam a restauração dos sistemas em casos de perdas.

Cabe ao *colaborador responsável pela informação* determinar quais são os ambientes críticos e, com o apoio da área de TI - Tecnologia da Informação, coordenar a elaboração, atualização e testes periódicos de Plano de Continuidade para os recursos computacionais de TI.

Devem ser estabelecidas formas e rotinas de *backups* que zelem por todas as informações corporativas armazenadas em meio magnético, utilizando as práticas mais adequadas disponíveis.

Todos os sistemas vigentes que gerem dados e informações críticas devem passar por rotinas de *backups* periódicos, de forma a garantir a manutenção da informação em caso de perda, dano ou roubo.

Sempre que ocorrerem mudanças consideradas significativas em sistemas operacionais e/ou *upgrades* devem ser executadas rotinas de *backup*.

As mídias derivadas dos *backups* devem ser armazenadas isoladamente, com acesso restrito às pessoas autorizadas e devidamente protegidas contrafogo, alagamento e semelhantes.

Todos os planos de contingência desenvolvidos deverão passar por testes, verificando sua funcionalidade e correção de eventuais desvios, devendo estar devidamente registrados e documentados.

2.14. CONTROLE DE ACESSO LÓGICO DOS USUÁRIOS

Cada colaborador, prestador de serviços ou fornecedor deve possuir, uma única conta (*username /login*) pessoal e intransferível, conforme o perfil de acesso definido, devendo os usuários ser identificados e registrados nos acessos aos recursos de informática.

O fornecimento de uma conta (*username/login*) para terceiros somente será cedido em casos específicos mediante aprovações.

Para elevar o nível de segurança dos acessos, os usuários devem definir para si senhas fortes como meio de validação de sua identidade quando dos acessos a estações de trabalho, redes, sistemas, servidores, etc., tal como recomendado pelas boas práticas de Segurança da Informação.

Toda concessão de acesso aos sistemas de TI deve ser efetuada de acordo com as necessidades de negócio, devendo ser previamente aprovada pelo gestor responsável em observância às regras estabelecidas para a gestão do sistema em questão.

O período de duração da concessão do acesso deve ser pertinente à função do usuário e de acordo com as orientações do *information owner (Responsável pela a Informação)*, devendo ser cancelada ao fim do contrato de prestadores de serviço e terceiros ou do desligamento do colaborador da PREVCOM.

Toda vez que uma conta de usuário (*username/login)* for cancelada, não deverá ser reutilizada, devendo os acessos a todos os sistemas vinculados à conta ser excluídos ou bloqueados. Uma exceção a essa regra será praticada quando um usuário (colaborador) for desligado e contratado novamente. Nesse caso ele receberá o mesmo *login* utilizado no passado (este cenário é específico para colaboradores).

Periodicamente, as contas dos usuários e seus privilégios nos aplicativos devem ser verificados ou atestados, de forma a promover a manutenção e atualização da base de cadastro, exclusão de usuários desligados, contas em desuso ou em duplicidade.

Todo acesso aos sistemas e aplicativos deve promover a sua correta autenticação utilizando-se seu *username/login* e senha, de forma a permitir a identificação individualizada do usuário preservando a rastreabilidade das ações.

Todos os sistemas que a área de Controles Internos definir como críticos para o negócio devem ser identificados e possuir trilhas de auditoria habilitadas, devendo ser registradas todas as operações privilegiadas, início e finalização do sistema, conexão e desconexão de dispositivos, tentativas de acesso não autorizadas, violação de *gateways* e *firewalls*, dentre outros.

2.15. SEGURANÇA EM MANUSEIO DE MÍDIAS

A utilização de mídias removíveis que permitem gravação, tais como: *pendrive, HD* Externo e gravador de CD ou DVD devem ser limitadas a diretores, gerentes e equipe de TI. Os demais colaboradores devem justificar a necessidade de uso para serem aprovadas pela Subcomissão de Segurança e Privacidade.

2.16. BYOD – USO DE EQUIPAMENTOS E DISPOSITIVOS PESSOAIS

A utilização de equipamentos pessoais conectados à rede corporativa da PREVCOM e suas Unidades de Negócio (Empresarial, Pessoal e Residencial & Combos), é permitido apenas em casos aprovados pelas diretorias da PREVCOM.

O acesso remoto de colaboradores autorizados em virtude de atividades de suporte e cargos de confiança somente deverá ser efetuado por meio de recursos liberados pela equipe de Infraestrutura de TI, onde existem controles de segurança implantados que podem garantir a confidencialidade e integridade das informações.

2.17. CLOUD COMPUTING

Toda a empresa contratada para a prestação do serviço de *cloud computing* deve disponibilizar a modalidade *Private Cloud* (Nuvem Privada), a fim de que possa assegurar a administração de itens como gerenciamento de redes, configurações do provedor, tecnologias de autenticação e autorização e criptografia dos dados transmitidos e armazenados possa ser realizada e/ou definida pela PREVCOM em normativo específico.

Deve haver no contrato de prestação do serviço de *cloud computing* itens que:

- Visem garantir a integridade, confidencialidade, disponibilidade, autenticidade e não-repúdio das informações manipuladas.
- Plano de Contingência dos Dados (incluindo recuperação de dados e administração de incidentes).
- ANS (Acordos de Nível de Serviço) e ANO (Acordo de Nível Operacional).
- Modelo de Gestão de Riscos.
- Garantir a gestão dos acessos conforme política de gestão de acesso lógico.
- Dever haver registro dos *logs* de acessos e *logs* de transações do sistema.

A empresa contratada deve garantir a segregação dos dados da contratante e oferecer total apoio em casos de investigação solicitado pela contratante, com prazos de retorno definidos em ANS.

2.18. TRATAMENTO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Todos os incidentes de segurança física e/ou lógica, ocorridos no âmbito da PREVCOM e suas Unidades de Negócios ou empresas prestadoras de serviço que estejam envolvidas no processamento de dados devem ser imediatamente comunicados às áreas responsáveis, por meio de canais apropriados, não sendo permitido qualquer tipo de investigação por outras áreas.

Todos os colaboradores, contratados e usuários terceirizados dos sistemas e serviços de AMBIENTE de TI regulamentados da PREVCOM devem ser obrigados a observar e relatar quaisquer fraquezas de segurança observadas ou suspeitas em sistemas ou serviços sem demora.

A equipe de TI detém autonomia para tomar decisões operacionais relacionadas aos incidentes de segurança, devendo requisitar a participação de qualquer colaborador ou fornecedor para auxiliar na análise e/ou resolução do incidente.

Todos os incidentes de segurança deverão ser classificados conforme grau de magnitude. Para casos extremos, deverá ser envolvida a Subcomissão de Segurança e Privacidade para gerir e registrar toda a situação, conforme normativo específico sobre o tema.

2.19. TRATAMENTO DE INCIDENTES DE SEGURANÇA DE DADOS PESSOAIS

Esta instrução tem como objetivo estabelecer as normas procedimentais em caso de incidentes de segurança de dados pessoais, com essa informação os colaboradores estarão preparados para:

- Classificar os dados envolvidos.
- Classificar a criticidade do incidente.
- Minimizar eventuais danos gerados para os titulares dos dados pessoais.
- Minimizar eventuais danos gerados para a PREVCOM.

Em caso de Incidentes, a resposta adequada será fundamental para a minimização dos danos causados aos titulares dos dados afetados e à PREVCOM.

As atividades relacionadas a estes incidentes seguem abaixo:

a) Reportar possíveis Incidentes de violação de dados pessoais prontamente.

b) O colaborador que notar um incidente desse tipo deve tomar nota dos eventos que o levaram a acreditar que um incidente esteja ocorrendo (data, hora, sistemas, computador ou pessoas afetadas/envolvidas).

c) O Encarregado de Dados será o responsável por monitorar estes alertas por parte de colaboradores e terceiros e fazer a análise inicial dos reportes recebidos, de forma imediata, juntamente com o gestor da área de Segurança da Informação.

d) A área de Segurança da Informação deverá conduzir, periodicamente, o monitoramento preventivo de sistemas, uso de web e mensagens de correio eletrônico, conforme descrito na Política de Segurança da Informação.

e) Caso o reporte inicial não contenha informações suficientes para a avaliação da ocorrência do incidente, o Encarregado de Dados ou o gestor da área de Segurança da Informação solicitará informações complementares ao informante.

f) Não havendo a existência de indícios razoáveis de que o incidente ocorreu, o reporte deverá ser formalizado em relatório e arquivado, indicando, ainda, as razões do arquivamento.

2.19.1. CLASSIFICAÇÃO DO INCIDENTE DE SEGURANÇA DE DADOS PESSOAIS

Constatada a ocorrência de um incidente, o Encarregado de Dados classificará o incidente conforme seu impacto no titular ou na PREVCOM e o tipo de dado envolvido.

Quanto ao tipo de dado, pode-se considerar a seguinte classificação:

- **Genérico:** Quaisquer informações relativas a uma pessoa singular identificada ou identificável, e que não esteja classificada abaixo como dados financeiros e/ou comportamentais.
- **Financeiro:** dados pessoais que remetam ou revelem qualquer aspecto da vida financeira do titular. Exemplos: número de conta, cartão de crédito, código verificador, renda, salário, benefícios.
- **Comportamental:** dados pessoais que demonstrem ou revelem o comportamento do titular. Exemplos: dados de localização, consumo, hábitos, preferências, endereço IP, cookies, logs de conexão, logs de acesso.
- **Sensível:** dados pessoais sobre origem racial, étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, referente à saúde, ou à vida sexual, Dado genético ou biométrico, quando vinculados a uma pessoa natural.

Considerando o impacto nas partes envolvidas, seja no titular ou na PREVCOM, é responsabilidade do Encarregado de Dados a notificação do Incidente para a ANPD e para os titulares, quando cabível.

2.19.2. RESPONSABILIDADES QUANTO AOS INCIDENTES DE SEGURANÇA DE DADOS PESSOAIS

Em linhas gerais, o Encarregado de Dados é responsável por:

- Identificar a causa raiz do incidente.
- Coordenar a resposta ao incidente.
- Assegurar que ocorra o menor tempo de reação entre a descoberta do incidente e o início do seu gerenciamento.
- Notificações e comunicações efetuadas sobre o incidente.
- Medir o impacto financeiro, reputacional e operacional do incidente, na PREVCOM.

É responsabilidade da Subcomissão de Privacidade e Segurança:

- Recomendar os posicionamentos públicos e estratégicos, relativos ao incidente.
- Alinhar o posicionamento e protocolos com a Diretoria Executiva da PREVCOM.
- Revisar todas as notificações de comunicação do incidente à ANPD e aos titulares dos dados.
- Auxiliar no posicionamento público da PREVCOM sobre o incidente, perante a imprensa, o mercado, colaboradores e parceiros da Fundação.
- Identificar obrigações contratuais e regulatórias de reportar o incidente para terceiros, órgãos reguladores/governamentais (que não a ANPD), elaborar e enviar as respectivas notificações.
- Auxiliar na elaboração de estratégias de compensação aos titulares de dados afetados, quando tal ação for necessária.

- Recomendar a contratação de assessoria externa jurídica, quando necessário, para apoio e consultoria para a resposta ao Incidente.
- Identificar o impacto do incidente no relacionamento com os colaboradores e processos de RH.
- Auxiliar na elaboração e divulgação das comunicações internas, quando necessário.

É responsabilidade do gestor de TI:

- Cessar a fonte de vazamento, se for o caso.
- Realizar a análise técnica do incidente.
- Realizar a detecção, isolamento, remoção e preservação dos sistemas afetados.
- Garantir que as evidências sejam mantidas para posterior perícia técnica.
- Contratar assessoria externa para apoiar em questões técnicas, se necessário.
- Auxiliar no levantamento das informações técnicas que deverão compor as notificações e comunicados a serem emitidos pela Fundação.

A Diretoria Executiva deverá:

- Aprovar o posicionamento da Fundação sobre o incidente, quando o mesmo repercutir na imprensa.
- Atuar como porta-voz da Fundação sobre o incidente, quando necessário.

2.20. VIOLAÇÃO DOS TERMOS DESSA POLÍTICA

Violações a esta política estão sujeitas às sanções disciplinares ou rescisão do contrato, observadas a natureza e a gravidade da infração, sendo passíveis de punições, e em conformidade com a legislação trabalhista, sem prejuízo de outras sanções penais e civis.

São consideradas também violações a esta política as seguintes situações:

- Não cumprimento das diretrizes e requisitos estabelecidos nas políticas de Segurança Corporativa da PREVCOM.
- Uso indevido e divulgação não autorizada de informações, segredos comerciais ou outras informações sem autorização formal do gestor da informação e da área de TI - Tecnologia da Informação (para garantir a forma correta de divulgação ou de disponibilização).
- Uso ilícito de dados, informações, equipamentos, sistemas e demais recursos tecnológicos, incluindo a violação de leis, regulamentos internos e externos e Código de Ética Corporativa da PREVCOM.
- Qualquer situação que exponha a PREVCOM a perdas financeiras ou comprometimentos de imagem, em decorrência da quebra da confidencialidade, integridade ou disponibilidade das suas informações ou das quais que detenham custódia.

2.21. DADOS PESSOAIS

A PREVCOM tem como uma de suas premissas a proteção dos dados pessoais de todas as pessoas envolvidas na sua cadeia de atividades. O direito à privacidade é uma prioridade e pauta todas as ações e políticas da PREVCOM. Dentre as atividades abrangidas por esta política, poderá ocorrer o tratamento/processamento de dados pessoais, ou seja, operações realizadas com dados pessoais, tais como, a coleta, produção, utilização, acesso, distribuição, processamento, arquivamento, eliminação, entre outros. Desta forma, qualquer tratamento de dados realizado deverá respeitar as disposições gerais desta Política, além dos demais documentos corporativos e políticas aplicáveis ao tema.

2.22. COMPETÊNCIAS

Gerência de TI - Tecnologia da Informação

- Coordenar as ações relacionadas à segurança da informação na PREVCOM.
- Dar ciência periódica, aos colaboradores e prestadores de serviço, sobre a Política de Segurança da Informação Corporativa.
- Ministrar treinamentos periódicos em segurança da informação.
- Responsabilizar-se pela definição das políticas e padrões de segurança da informação da PREVCOM.
- Apoiar os gestores das informações na definição de regras e procedimentos de concessão de acessos.
- Garantir que a segurança da informação seja parte do processo de planejamento da informação no âmbito de TI.
- Executar o controle dos acessos aos sistemas garantindo que o processo de concessão, revogação e alteração dos acessos seja cumprido.
- Implantar ferramentas de segurança no ambiente de infraestrutura com o objetivo de garantir a confidencialidade, disponibilidade e integridade das informações.
- Elaborar procedimentos necessários para adequação dos ativos ao nível de segurança pertinentes às políticas e demais normativos da PREVCOM.
- Tratar os incidentes de Segurança da Informação, no âmbito de TI.
- Apoiar e acompanhar as auditorias internas e externas de Segurança da Informação realizadas por clientes ou órgãos reguladores.
- Aprovar as solicitações de acessos a sistemas/informações de seus subordinados, ou prestadores de serviços sob sua responsabilidade.
- Solicitar e/ou aprovar a concessão de acessos a usuários da informação de acordo com as regras definidas pelo gestor da informação, diretorias ou outras áreas custodiantes.

Diretoria de Tecnologia da Informação ou Outras Áreas Custodiantes

- Proteger e gerenciar os ativos de computação disponibilizados pela PREVCOM assegurando mecanismos para proteção adequada das informações de acordo com sua respectiva classificação.
- Disponibilizar os acessos de acordo com as diretrizes definidas pelo gestor da informação.

- Fornecer os recursos para recuperação das informações.
- Apoiar os gestores das informações junto aos processos de monitoramento.

Gestor ou dono da Informação

- Classificar ativos da informação de acordo com a sua natureza conforme norma especificada por Segurança da Informação Corporativa.
- Estabelecer regras de proteção dos ativos de informação.
- Especificar condições para a realização de cópias de segurança.
- Aprovar novos desenvolvimentos ou manutenções que sejam de natureza evolutiva, corretiva ou novos projetos, assim como validação para sua entrada em produção.
- Apurar, com o apoio das áreas custodiantes, violações registradas e participar das ações a serem tomadas, quando da ocorrência de uma não conformidade.
- Revisar periodicamente a concessão de acessos às informações sob sua responsabilidade.

Gestor de Acesso

- Aprovar as solicitações de acessos a sistemas/informações dos empregados ou prestadores de serviços sob sua responsabilidade.
- Solicitar os cancelamentos de acessos de empregados ou prestadores de serviços que não necessitem mais do acesso no exercício de suas atribuições.
- Revisar periodicamente os acessos dos usuários da informação sob sua reponsabilidade, solicitando qualquer alteração de acessos que se faça necessária.
- Efetuar a delegação de autoridade, alçadas de aprovações para pagamentos de despesas, investimentos, movimentações financeiras e organizacionais, quando estiver ausente por motivos de férias ou licença.

Usuários da Informação

- Usar adequadamente as informações disponibilizadas.
- Manter o sigilo de suas senhas.
- Guardar de forma segura os materiais considerados estritamente confidenciais ou de uso interno.
- Comunicar a área de TI - Tecnologia da Informação de todo e qualquer desvio às normas de Segurança da Informação da PREVCOM.
- Contribuir para a melhoria dos níveis de Segurança da Informação.

2.23. REFERÊNCIAS

- POLÍTICAS DE GOVERNANÇA CORPORATIVA E CÓDIGO DE ÉTICA.
- **ABNT NBR ISO/IEC 27001:2013:** Tecnologia da Informação — Técnicas de Segurança — Sistemas de Gestão da Segurança da Informação — Requisitos.
- **ABNT NBR ISO/IEC 27002:2005 –** Tecnologia da Informação: Técnicas de Segurança – Diretrizes para Implantação de Um Sistema de Gestão da Segurança da Informação.
- **ABNT NBR ISO/IEC 27011:2005 –** Tecnologia da Informação: Técnicas de Segurança - Gestão da Segurança da Informação em Organizações de Telecomunicações.

2.24. GLOSSÁRIO

- **APROVADOR:** Pessoa formalmente autorizada pelo gestor da informação para aprovação da concessão de acessos.
- **ÁREAS CUSTODIANTES:** Áreas delegadas pelos gestores das informações "I/O - Information Owners" que, por definição da Fundação, tem autonomia em relação ao ciclo de vida de aquisição, desenvolvimento e manutenção dos sistemas.
- **ATIVO DE INFORMAÇÃO:** Toda informação, não importando a mídia que a suporte e que represente valor para os negócios da Fundação de Previdência Complementar do Estado de São Paulo.
- **AUTENTICIDADE:** Propriedade da informação que confirma a originalidade de seu conteúdo, comprovando sua origem e sua autoria.
- **AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS ("ANPD"):** Órgão pertencente à administração pública federal, responsável pela fiscalização do cumprimento das disposições da Lei Geral de Proteção de Dados.
- **BYOD (BRING YOUR OWN DEVICE):** Conceito que permite o uso de dispositivos móveis pessoais para exercer suas atividades no ambiente de trabalho conforme normas e requisitos estabelecidos pela Fundação.
- **CLOUD COMPUTING:** Computação (sistemas, banco de dados, aplicação, etc.) em nuvem, ou seja, é a entrega de serviços de TI onde o acesso é possível por meio de qualquer dispositivo, estando dentro ou fora da rede da Fundação e empregando a internet como meio de comunicação.
- **COLABORADOR (ES):** São todos os empregados e funcionários da PREVCOM, incluindo conselheiros e diretores.
- **CONFIDENCIALIDADE:** Propriedade da informação que garante que o conteúdo é acessível somente por pessoas autorizadas.
- **CONTAS / LOGIN:** Identificação de um usuário na rede corporativa, aplicativos ou outros recursos de processamento de informações.
- **CONTROLADOR:** Parte que determina as finalidades e os meios de Tratamento de dados pessoais.
- **DADOS COMPORTAMENTAIS:** dados pessoais que demonstrem ou revelem o comportamento do titular. Exemplos: dados de localização, consumo, hábitos, preferências, endereço IP, cookies, logs de conexão, logs de acesso.
- **DADOS FINANCEIROS:** dados pessoais que remetam ou revelem qualquer aspecto financeiro do titular. Exemplos: número de conta, cartão de crédito, senha, código verificador, renda, salário, benefícios.

- **DADOS PESSOAIS SENSÍVEIS:** dados pessoais sobre origem racial, étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, referente à saúde, ou à vida sexual, dado genético ou biométrico, quando vinculados a uma pessoa natural.
- **DADOS PESSOAIS:** Quaisquer informações relativas a uma pessoa singular identificada ou identificável. é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrônica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, econômica, cultural ou social dessa pessoa singular.
- **DAR:** Documento de Aceitação de Riscos, utilizado para formalizar os riscos de determinado projeto ou situação.
- **DISPONIBILIDADE:** Propriedade da informação que garante que usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.
- **ENCARREGADO DE DADOS:** Pessoa indicada pelo Controlador e Operador para atuar como canal de comunicação entre o Controlador, os titulares dos Dados e a Autoridade Nacional de Proteção de Dados (ANPD).
- **FRAUDE:** Subterfúgio para alcançar um fim ilícito e/ou engano dolosamente provocado, induzimento ao erro ou aproveitamento de preexistente erro alheio.
- **GESTOR DA INFORMAÇÃO ("INFORMATION OWNERS"):** Diretores ou níveis hierárquicos acima, responsáveis pelas informações geradas e/ou manuseadas para realização dos processos de negócio da Fundação de Previdência Complementar do Estado de São Paulo.
- **GESTOR DE ACESSOS:** Pessoa formalmente nomeada para apoio na implementação das regras de aprovação e concessão de acessos.
- **INCIDENTE DE SEGURANÇA DE INFORMAÇÕES:** Qualquer evento que afete ou possa afetar, de forma prejudicial e/ou maliciosa, os negócios e/ou a integridade física e/ou lógica dos ambientes da Fundação de Previdência Complementar do Estado de São Paulo.
- **INCIDENTES:** Acesso, aquisição, uso, compartilhamento, destruição, alteração ou indisponibilidade de dados pessoais, proposital ou acidental, não autorizada ou ilícita. Violação da confidencialidade, integridade e disponibilidade de dados pessoais. Exemplos: Perda de laptop com dados pessoais de colaboradores, que não estejam criptografados. Envio de e-mail que contenha dados pessoais de clientes para o destinatário errado. Arquivo de currículos de candidatos a uma vaga exposto em um diretório aberto na internet, com acesso sem necessidade de identificação (usuário e senha). Extração de dados pessoais de servidores da Fundação por um terceiro que utilize de falhas técnicas e engenharia social ("ataque hacker").
- **INFORMAÇÕES CORPORATIVAS:** Informações direta ou indiretamente envolvidas na operação dos sistemas corporativos da Fundação de Previdência Complementar do Estado de São Paulo, independentemente do local onde tenham sido produzidas.
- **INFORMATION OWNER:** Responsável (gestor) das informações de um sistema ou módulo do sistema.
- **INTEGRIDADE:** Propriedade da informação que garante a salvaguarda da exatidão e completude da informação.
- **LEGALIDADE:** Propriedade que garante que a informação se encontra em concordância com as legislações vigentes e aplicáveis a Fundação de Previdência Complementar do Estado de São Paulo.
- **MESA LIMPA:** Prática na qual, ao final do expediente, os documentos considerados confidenciais ou uso interno são armazenados em locais seguros, tais como: armário e gavetas disponíveis com chaves.

- **NÃO REPÚDIO:** Propriedade da informação em que o autor não pode negar a responsabilidade sobre ele atribuída. Consegue-se estabelecer a característica de não repúdio com a combinação de confidencialidade e integridade da informação.
- **OWASP (OPEN WEB APPLICATION SECURITY PROJECT):** Entidade dedicada a capacitar organizações para conceber, desenvolver, adquirir, operar e manter aplicações que precisam ser confiáveis para desenvolvimento de aplicações *web*.
- **PERFIL DE ACESSO:** Conjunto de permissões definidas em um sistema ou aplicativo focado nas necessidades de um determinado posto de trabalho ou cargo seguindo as necessidades do negócio.
- SEGREGAÇÃO DE FUNÇÕES: Princípio básico de controle que consiste na separação de funções, normalmente de autorização, aprovação, execução e controle, de tal forma que nenhuma pessoa, pelo acúmulo de privilégios, detenha competências em desacordo com este princípio.
- **SEGURANÇA DA INFORMAÇÃO:** Conjunto de medidas que visam a preservação da confidencialidade, integridade, autenticidade, legalidade e disponibilidade das informações.
- **SEGURANÇA FÍSICA E PATRIMONIAL:** Conjunto de medidas que têm por objetivo a proteção contra ocorrências, visando evitar, conter e/ou minimizar atos deliberados que possam ou não causar danos às pessoas, ao patrimônio, às informações, à execução dos serviços ou à imagem da Fundação de Previdência Complementar do Estado de São Paulo.
- **SENHA FORTE:** Conjunto de caracteres recomendados que, quando da verificação da identidade de um usuário, gera maior segurança e proteção contra *hackers, softwares* maliciosos etc..
- **SISTEMA DE CONTROLE DE ACESSO:** Sistema de controle que garante que os acessos sejam efetuados apenas por pessoas autorizadas.
- **SISTEMA DE INFORMAÇÃO:** Conjunto de informações relacionadas, de modo a formar uma base de conhecimento sobre um processo, suportada ou não por programas de computador.
- **SYSTEM OWNER DE INFRA/APLICAÇÃO:** Responsável técnico pelo funcionamento do sistema/aplicação.
- **TERCEIROS:** São todos os prestadores de serviços, trabalhadores terceirizados, parceiros comerciais, fornecedores e representantes da PREVCOM.
- **TESTES DE SEGURANÇA:** Testes a serem aplicados aos sistemas de informação visando à validação sobre o atendimento dos requerimentos de segurança.
- **TITULAR DOS DADOS:** Pessoa natural a quem se referem os dados pessoais objeto de tratamento pela PREVCOM.
- **TRATAMENTO:** Qualquer operação ou conjunto de operações efetuadas com dados pessoais ou sobre conjuntos de dados pessoais por meios automatizados ou não automatizados, tais como a coleta, o registro, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, a eliminação ou a destruição
- **USERNAME:** Chave única de identificação do usuário para acesso à rede, correio eletrônico e sistemas, também conhecido como *login*.
- **USUÁRIO DA INFORMAÇÃO:** Pessoa que tem como papel utilizar-se das informações da Fundação de Previdência Complementar do Estado de São Paulo no desempenho de suas atividades e em conformidade com a política e normas de segurança da informação.

3. POLÍTICA DE RELACIONAMENTO COM FORNECEDORES

3.1. OBJETIVO

Definir critérios e diretrizes para orientar as atividades decorrentes do relacionamento entre a PREVCOM e seus fornecedores.

3.2. APLICAÇÃO

Para fins desta norma, a referência à empresa Fundação de Previdência Complementar do Estado de São Paulo está sendo feita como “PREVCOM” ou “Fundação”.

3.3. RESPONSABILIDADES

- Diretoria.
- Gerência de Tecnologia da Informação – TI.
- Todos os colaboradores envolvidos com o tema.

3.4. CONCEITUAÇÃO

CONFLITO DE INTERESSES: Situações nas quais a atuação do funcionário ou fornecedor indica a busca de quaisquer vantagens e/ou benefícios próprios ou de terceiros, em detrimento dos interesses da Fundação.

FORNECEDOR: Toda pessoa física ou jurídica, pública ou privada, nacional ou estrangeira, bem como os entes despersonalizados, que desenvolvem atividades de produção, montagem, criação, construção, transformação, importação, exportação, distribuição ou comercialização de produtos ou prestação de serviços à Fundação, necessários e utilizados na execução do objeto social da Fundação.

MATERIAIS, BENS E SERVIÇOS: Qualquer bem, móvel ou imóvel, material ou imaterial, assim como qualquer atividade fornecida mediante remuneração, que são adquiridos pela PREVCOM.

REQUISITANTE: Responsável por emitir a requisição de compras necessária para solicitar a contratação de um material ou serviço.

3.5. ASPECTOS GERAIS

Toda relação de funcionários da Fundação com fornecedores deve ser realizada de forma ética e profissional, em conformidade com o Código de Ética da Fundação, mantendo-se os níveis adequados de exigência, transparência e zelo com relação aos critérios estabelecidos pela Fundação.

3.6. RELACIONAMENTO EMPRESA X FORNECEDORES

Todos os fornecedores devem ser tratados igualmente, sem preferência durante as etapas do processo de licitação e de contratação de materiais, bens ou serviços, que deve ser sempre conduzido pela ou sob a gerência da área de Suprimentos e Suporte Logístico ou, nos casos especiais de alçadas deslocadas, pelas respectivas diretorias definidas na Política de Alçadas.

Somente os funcionários da área de Suporte Logístico e Suprimentos e os citados na alínea acima, estão autorizados a solicitar propostas comerciais e negociar com fornecedores.

Todas as negociações de caráter técnico podem contar com a participação da área requisitante, cabendo a negociação comercial ser efetuada, exclusivamente, pela área de Suporte Logístico e Suprimentos.

A área de Suporte Logístico e Suprimentos e a Diretoria Administrativa quando necessário deve ser convidada a participar de qualquer reunião com o fornecedor que tenha como objetivo desenvolver projetos para futuras contratações, cabendo exclusivamente a mesma decidir quanto a sua participação.

Todas as informações compartilhadas entre a PREVCOM e seus fornecedores devem ser consideradas como confidenciais. Portanto, não devem ser reveladas ou utilizadas para uso diferente do estabelecido nos respectivos contratos.

O relacionamento comercial com os fornecedores deve ser estabelecido com base em sua qualificação e competência, sem favoritismo ou tendência, devendo ser considerado na escolha, entre outros fatores objetivos, o valor, a qualidade, o prazo de entrega e o custo dos produtos e serviços oferecidos.

O único documento reconhecido pela empresa que caracteriza a formalização de uma negociação e seu posterior pagamento é o Ofício de Reserva da Disponibilidade Orçamentária devidamente autorizado pelo Diretor Presidente/Diretoria administrativa ou nos casos especiais de alçadas deslocadas.

Nenhum funcionário da PREVCOM tem autorização para solicitar que um fornecedor inicie a instalação de qualquer equipamento, entrega de materiais, bens ou serviços a PREVCOM, sem estar de posse do respectivo Contrato/Pedido devidamente autorizado, liberado e assinado, por aqueles que possuem poderes para tanto, exceto quando autorizado formalmente pela área de Suporte Logístico e Suprimentos/Diretoria administrativa.

Todos os pedidos de compras somente devem ser autorizados no sistema após o recebimento do contrato formal devidamente assinado entre as partes envolvidas com poderes formais para tal ato.

Todo convite realizado por fornecedores para participação em seminários, eventos técnicos, cursos, visitas técnicas a escritórios, independentemente da finalidade, deverá ser encaminhado para o Órgão de Recursos Humanos para aprovação do diretor do órgão.

Toda e qualquer publicação ou anúncio público relativo à aquisição de materiais, bens e serviços para a PREVCOM via pregões eletrônicos, licitações, tomadas de preço, emissão de *RFP (request for proposals*) ou semelhantes devem ser sempre e previamente aprovados pela Diretoria Administrativa.

3.7. RELACIONAMENTO FORNECEDORES X FUNCIONÁRIOS

Todo atendimento a Fornecedores deve ser realizado com caráter igual e institucional, nunca de forma pessoal.

Todo relacionamento de funcionários da PREVCOM com Fornecedores deve ser realizado e mantido com especial exigência e cuidado, balizado sempre na transparência e apego estrito às sistemáticas estabelecidas pela PREVCOM.

Os funcionários da PREVCOM devem evitar, com todos os Fornecedores, estabelecer um relacionamento, seja no âmbito pessoal ou comercial, que possa vir a caracterizar situações de Conflitos de Interesses ou afetar o julgamento imparcial e objetivo dessas eventuais situações.

Não é permitido ao funcionário da PREVCOM participar de negociações (técnicas ou comerciais) com pessoas ligadas aos Fornecedores que possuírem qualquer grau de parentesco e/ou vínculo matrimonial. Nestes casos, o responsável superior do funcionário deve ser comunicado imediatamente e a responsabilidade de negociação deve ser transferida para outro funcionário que não se enquadre nestas hipóteses.

Se algum funcionário da PREVCOM perceber a existência de alguma relação suspeita entre Fornecedores e funcionários da PREVCOM, que possa ser caracterizada como Conflito de Interesses, deverá utilizar o canal de comunicação do Código de Ética, disponibilizado na Intranet da companhia, informando sobre a situação existente.

Não devem ser aceitos pelos funcionários da PREVCOM convites para almoços, jantares, confraternizações, nem mesmo por meio do fornecimento de vouchers ou o recebimento de quaisquer tipos de presentes ou favores. Exceção é feita para brindes simbólicos sem valor comercial (materiais promocionais com a logomarca da empresa Fornecedora ou representante) como por exemplo, calendários, canetas, copos, blocos e semelhantes.

Sempre que um brinde recebido não atender a qualquer um dos critérios de permissão (valor simbólico, material promocional com a logomarca do Fornecedor) ou ensejar interpretações duvidosas, a situação deverá ser imediatamente submetida à Área de Contratação de Suprimentos, para análise e definição das ações a serem adotadas.

3.8. ASPECTOS FINANCEIROS E COMERCIAIS

Todas as cobranças de multa que a PREVCOM venha a **sofrer** referente a qualquer situação contratual com Fornecedores, só poderão ter seu pagamento realizado mediante parecer prévio e favorável da Diretoria Executiva Corporativa e o “de acordo” do Diretor Executivo de Suprimentos, salvo em casos excepcionais definidos e autorizados pela Presidência. Os valores destas multas deverão ser alocados no Centro de Custo da área requisitante do serviço.

Caberá ao Requisitante (Gestor do Contrato) responsável pelo serviço, providenciar a emissão da “Folha de Registro” no SISTEMA, no mês da realização do serviço, que expressa: o aceite, o registro na contabilidade, a aprovação e a autorização do pagamento. A ausência da "Folha de Registro" impossibilita a Gerência de Contas a Pagar de lançar a nota fiscal no SISTEMA.

Todos os pagamentos devem ser feitos em conformidade com as condições contratualmente estabelecidas, desde que as notas fiscais sejam entregues à Gerência de Contas a Pagar até a data estabelecida no “Calendário de Pagamentos a Fornecedores do PREVCOM" e satisfaçam as condições estabelecidas.

Na hipótese de haver necessidade de antecipação do cronograma físico por solicitação da PREVCOM, o pagamento da respectiva parcela poderá ser antecipado e efetuado em conformidade com as sistemáticas vigentes. Todavia, caso a solicitação de antecipação ocorra por requerimento do Fornecedor, o pagamento da respectiva parcela poderá, a critério exclusivo da PREVCOM, ser antecipado, inclusive com a aplicação de desconto financeiro a ser calculado com base nas taxas praticadas à época no mercado e acertado com o Fornecedor. Em não havendo concordância desta solicitação pela PREVCOM, o pagamento será efetuado conforme originalmente previsto no Pedido.

3.9. EXCEÇÕES

Não se aplica.

3.10. REFERÊNCIAS

- Código de Ética de PREVCOM.
- Quaisquer normas de suprimentos / compras.
- Política de Privacidade.
- Política de Privacidade de Colaboradores.

4. POLÍTICA DE PRIVACIDADE PROTEÇÃO DE DADOS PESSOAIS E COOKIES

4.1. OBJETIVO

Trata-se das diretrizes adotadas pela PREVCOM em relação à recepção, coleta e tratamento dos dados pessoais disponibilizados pelos clientes e visitantes, para acesso e uso dos nossos serviços (sites institucionais e de serviços da PREVCOM, denominados "serviços"), que necessitam de identificação.

Salientamos que a presente Política não se aplica ao tratamento, por parte da PREVCOM, dos dados pessoais dos funcionários, trabalhadores temporários ou outros funcionários da PREVCOM em relação às funções que desempenham para a PREVCOM. Há uma política de privacidade independente que rege este tratamento.

4.2. RESPONSABILIDADES

- Diretoria.
- Gerência de Tecnologia da Informação – TI.
- Todos os colaboradores envolvidos com o tema.

4.3. TERMOS E CONDIÇÕES

Para fins desta política, a referência à empresa Fundação de Previdência Complementar do Estado de São Paulo está sendo feita como “PREVCOM” ou “Fundação”.

Todos os termos e condições constantes na presente Política de Privacidade poderão ser modificados ou atualizados a qualquer momento pela PREVCOM, em virtude de alterações na legislação ou nos serviços, em decorrência da utilização de novas ferramentas tecnológicas ou, ainda, sempre que, a exclusivo critério da Fundação, tais alterações se façam necessárias. Diante do exposto, recomendamos aos nossos usuários e clientes que, previamente à utilização dos serviços disponíveis, seja verificada a Política de Privacidade então vigente. A utilização dos serviços disponibilizados pela PREVCOM para qualquer usuário ou cliente implicará em expressa aceitação quanto aos termos e condições da Política de Privacidade vigente na data de sua utilização. Recomendamos àqueles usuários e clientes que não concordam com a Política de Privacidade vigente, a não utilização dos serviços da Fundação, visto que a sua não aceitação ou ainda, a não disponibilização das informações solicitadas, pode impedir a prestação de tais serviços. Ao utilizar qualquer Site, Aplicativo ou Dispositivo da PREVCOM, considera-se que o usuário/cliente aceitou esta Política. Se não aceitar os termos estabelecidos na presente Política, não deverá utilizar Sites, Aplicativos ou Dispositivos.

Ressaltamos que novos serviços online, disponibilizados pela Fundação, estarão automaticamente sujeitos à Política de Privacidade vigente à época de sua utilização.

4.4. CONCEITUAÇÃO – TRATAMENTO DE DADOS PESSOAIS

Para o fornecimento dos serviços, a Fundação adota recursos avançados visando a proteção dos dados pessoais dos usuários. A categoria de dados pessoais que podem ser tratados pela PREVCOM para atendimento das finalidades legais ou contratuais decorrente de relação estabelecida, incluem, mas não se limitam: nome completo do cliente/usuário, endereço físico e eletrônico, número de telefone, RG, CPF, número de cartão de crédito, situação financeira, patrimonial, , preferências e padrões de acesso ("dados pessoais") , os quais não são divulgadas pela Fundação, exceto nas hipóteses expressamente mencionadas neste documento.

Tais informações são coletadas por meio dos canais de atendimento e armazenadas, utilizando-se rígidos padrões de sigilo e integridade, bem como controles de acesso físico e lógico, observando-se sempre os mais elevados princípios éticos e legais.

Finalidades para as quais a PREVECOM pode tratar os dados pessoais:

Caso o usuário decida fornecer seus dados pessoais, tal ato implicará em expressa autorização para que tais informações sejam utilizadas para as seguintes finalidades, em particular, na medida permitida pela Lei:

- o fornecimento dos serviços, com o propósito definido em contrato de prestação de serviços assinado ou de procedimentos preliminares relacionados a um contrato, bem como para que tais informações sejam arquivadas.
- para monitorizar, adaptar, atualizar, proteger e melhorar os serviços que oferecemos.
- para verificar a identidade do titular e garantir a segurança dos seus dados pessoais no sentido de assegurar a sua correta identificação.
- para responder aos seus pedidos e necessidades de apoio.
- para entender a forma como as pessoas utilizam coletivamente os recursos de um site, aplicativo ou dispositivo (ou veículo associado).
- para administrar conteúdo, promoções, questionários ou outros recursos de um Site, Aplicativo ou Dispositivo.
- para lhe enviar comunicações sobre a administração das suas contas e das funcionalidades de um Site, Aplicativo ou Dispositivo.
- para o informar sobre alterações de um Site, Aplicativo ou Dispositivo.
- para realizar análises de tendências e análise financeira para a execução de um contrato ou contrato futuro.
- para dar efeito aos seus direitos legais e aos seus direitos no âmbito da presente Política.
- para proteção contra fraude, roubo de identidade e outras atividades ilegais no cumprimento da relação estabelecida, seja no âmbito comercial ou já contratual.
- para estabelecer ou exercer os direitos legais da PREVCOM ou defender reivindicações legais.
- para cumprir as Leis Aplicáveis e as nossas outras políticas aplicáveis.

Uma vez provido dos dados pessoais do usuário/cliente, a Fundação poderá utilizar os dados para o fim de entrar em contato com o usuário/cliente para fornecer informações, direcionadas por e-mail ou por quaisquer outros meios de comunicação, contendo informações sobre a Fundação, seus produtos e serviços que possam ser do seu interesse.

Entretanto, fica reservado ao usuário/cliente o direito de, a qualquer momento, inclusive no ato da disponibilização das informações pessoais, informar a Fundação por meio dos canais de comunicação disponíveis para o cadastramento de tais informações, do não interesse em recebe-las, inclusive por e-mail, hipótese em que a Fundação interromperá tais serviços e informações no menor tempo possível, ou ainda por meio do nosso Encarregado, conforme e-mail descrito no item ‘’Dados de Contato’’ desta política.

Proteção dos dados pessoais

Para que as atividades de tratamento de dados pessoais ocorram da maneira correta, nos termos pretendidos pela PREVCOM e conforme a lei de proteção de dados pessoais, os colaboradores e terceiros envolvidos no tratamento de dados pessoais devem:

- Tratar somente os dados necessários para o cumprimento da finalidade pretendida.
- Garantir o cumprimento dos direitos dos titulares.
- Ser transparente sobre suas atividades de tratamento de dados pessoais para com os titulares dos dados.
- Tratar os dados com ética e respeito ao titular, sem fins discriminatórios ou ilícitos.
- Implementar práticas adequadas de tratamento de dados e medidas de segurança técnicas e organizacionais adequadas para garantir a segurança dos dados pessoais e proteger contra acesso não autorizado, alteração, divulgação ou destruição.
- Consultar ou o Encarregado de Dados ou o comitê de privacidade em caso de dúvidas sobre o tratamento de dados.
- Reportar ao Encarregado de dados qualquer suspeita de violação de dados pessoais.
- Coletar, utilizar, armazenar, compartilhar e descartar dados pessoais de acordo com nossas políticas e procedimentos.

A Internet não é, por si só, um ambiente seguro e não podemos fornecer uma garantia absoluta de que os seus dados pessoais transferidos pela Internet estarão sempre protegidos. A transmissão de dados pessoais pela internet é de responsabilidade do titular, que apenas deve utilizar sistemas seguros para acessar a sites, aplicativos ou dispositivos.

O titular de dados é responsável por manter as suas credenciais de acesso a cada site, aplicativo e dispositivo seguras e confidenciais. Deve alterar frequentemente as suas credenciais de acesso e deve notificar a PREVCOM imediatamente se tomar conhecimento de qualquer utilização indevida das suas credenciais de acesso e mudá-las imediatamente.

4.5. DIVULGAÇÃO DOS DADOS PESSOAIS

O acesso aos dados pessoais tratados pela PREVCOM é restrito aos profissionais autorizados ao uso direto dessas informações e necessário à prestação de seus serviços, sendo limitado o uso para outras tarefas. É exigido, também, de toda organização ou indivíduo contratado para a prestação de serviços de apoio, que sejam cumpridas as Políticas de Segurança da Informação e o Código de Ética adotado pela PREVCOM.

A PREVCOM poderá compartilhar ou divulgar os dados pessoais que tenha recebido, concordando, desde já, o usuário com tal compartilhamento ou divulgação, nas seguintes hipóteses:

- sempre que estiver obrigado a revelá-las, seja em virtude de dispositivo legal, ato de autoridade competente, ordem ou mandado judicial.
- aos seus parceiros comerciais e/ou prestadores de serviço, a fim de atender à solicitação de serviços efetuada pelos usuários, operações do site, aplicativos ou dispositivos.
- aos colaboradores da PREVECOM, na medida do necessário para prestação dos serviços e cumprimento de obrigação legal.
- aos órgãos de proteção e defesa de crédito e prestadores de serviços autorizados pelo banco a defender seus direitos e créditos.

- aos órgãos que administrem cadastros de consumidores.
- aos seus controladores, às empresas por ele controladas, as empresas a ele coligadas ou por qualquer forma associadas, no Brasil ou no exterior.
- para instituições financeiras, para operacionalizar e facilitar pagamentos, desde que dentro dos parâmetros legais estabelecidos para tanto, podendo, nesta hipótese, o usuário, a qualquer tempo, revogar esta autorização.

A participação da Fundação no processo é revisar as informações, valores e informativos e enviar para o usuário, um comunicado de qualquer discrepância nas informações fornecidas.

4.6. TRANSFERÊNCIAS INTERNACIONAIS DE DADOS PESSOAIS

A PREVCOM, conforme finalidade definida em cada relacionamento estabelecido com o usuário e cliente, poderá utilizar instalações de tratamento de dados controlados ou operados pelos nossos prestadores de serviços terceirizados localizados em jurisdições diferentes da jurisdição em que os seus dados pessoais foram originalmente recolhidos. Especificamente, o conteúdo e os recursos de um Site, aplicativo ou Dispositivo podem ser fornecidos por meio de servidores localizados fora da sua jurisdição (incluindo, entre outros, servidores localizados nos Estados Unidos). Os dados pessoais podem ser transferidos e tratados utilizando esses servidores como parte da operação de um Site, aplicativo ou Dispositivo ou em associação a qualquer uma das finalidades de tratamento indicadas na presente Política, sempre em conformidade com as disposições das Leis Aplicáveis. Essas transferências são necessárias para fornecer os nossos produtos e serviços de forma eficiente e eficaz. Ao fornecer dados pessoais à PREVCOM no âmbito da presente Política de Privacidade, o usuário reconhece que os seus dados pessoais podem ser transferidos para locais fora da sua jurisdição. Se não quiser que os seus dados pessoais sejam transferidos para outras jurisdições, não forneça os seus dados pessoais à PREVCOM nem utilize Sites, Aplicativos ou Dispositivos.

Se transferirmos os seus dados pessoais para outros países, a transferência será realizada sempre respeitando essa Política, as cláusulas contratuais ajustadas entre as Partes e a LGPD. A PREVCOM, dentro do seu conhecimento, transferirá os dados apenas para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado e sempre de acordo com as cláusulas contratuais específicas ajustadas entre as Partes, se for o caso.

4.7. EXTENSÃO DOS EFEITOS

Os termos da Política de Privacidade aqui expostos serão aplicados exclusivamente aos dados pessoais, conforme acima definido, que venham a ser disponibilizadas a PREVCOM, pelo usuário para a utilização de seus produtos e serviços.

Por consequência, a Política de Privacidade aqui exposta não será aplicável a outro serviço que não os disponibilizados pela PREVCOM, incluídos aqueles sites que estejam de alguma forma vinculados ao site da Fundação, por meio de links ou quaisquer outros recursos tecnológicos, e, ainda, a quaisquer outros sites que, de alguma forma, venham a ser conhecidos ou utilizados pela Fundação.

Nesse sentido, alertarmos aos usuários que os referidos sites podem conter política de privacidade diversa da adotada pela PREVCOM ou podem até mesmo não adotar qualquer política nesse sentido, não se responsabilizando, a Fundação, por qualquer violação aos direitos de privacidade dos usuários que venham a ser violados pelos referidos sites.

4.8. DIREITOS AUTORAIS

A PREVCOM assegura que as informações (textos, imagens, sons e/ou aplicativos) contidas nos seus sites estão de acordo com a legislação e normativos que regulam os direitos autorais, marcas e patentes, não sendo permitidas modificações, cópias, reproduções ou quaisquer outras formas de utilização para fins comerciais sem o consentimento prévio e expresso da Fundação.

A PREVCOM não se responsabiliza por eventuais danos e/ou problemas decorrentes da demora, interrupção ou bloqueio nas transmissões de dados ocorridos na internet.

4.9. TÉRMINO DO TRATAMENTO DE DADOS PESSOAIS

A PREVCOM encerrará o tratamento dos seus dados pessoais nas seguintes hipóteses:

- quando a finalidade foi alcançada ou os dados deixaram de ser necessários conforme essa Política.
- quando o prazo necessário para o tratamento for alcançado.
- quando o usuário solicitar a exclusão dos Dados.
- por determinação da autoridade nacional de proteção de dados ou outra autoridade legalmente constituída.

O usuário tem ciência de que, mesmo após o término do tratamento de dados, a PREVCOM poderá manter os dados pessoais para as seguintes finalidades:

- cumprimento de obrigação legal ou regulatória.
- transferência à terceiros, quando o caso.
- uso anonimizado pela PREVCOM.

4.10. DADOS DE CONTATO

Se o usuário tiver qualquer dúvida ou preocupação sobre esta Política de Privacidade, nossas práticas de coleta e uso de dados pessoais, ou sobre uma possível violação de dados pessoais ou privacidade, entre em contato com a PREVCOM, por meio do seguinte e-mail: privacidade.prevcom@sp.gov.br.

Se o usuário nos contatar, tentaremos investigar e resolver cada questão ou reclamação no prazo de 15 dias ou em qualquer outro período exigido pelas leis aplicáveis.

4.11. LEI APLICÁVEL E RESOLUÇÃO DE CONFLITOS

Toda e qualquer controvérsia oriunda dos termos expostos na presente Política de Privacidade serão solucionados de acordo com a lei brasileira, sendo competente o foro da cidade de São Paulo, SP, comarca da Capital, com exclusão de qualquer outro por mais privilegiado que seja.

Fica claro, ainda, que utilização de serviços e as ordens comandadas fora do território brasileiro, ou ainda as decorrentes de operações iniciadas no exterior podem estar sujeitas também à legislação e jurisdição das autoridades dos países onde forem comandadas ou iniciadas.

4.12. DISPOSITIVOS MÓVEIS

Para utilização do app da PREVCOM são obrigatórios três tipos de autorizações, descritas abaixo:

1. Localização. Necessário para envio de pushs personalizados e funcionamento do localizador de agências. A Fundação pode usar a sua localização para prevenção a fraudes.
2. Telefone (fazer e gerenciar chamadas telefônicas). Necessário para identificação do dispositivo. A Fundação armazena o nome do telefone e seu ID (IMEI), apenas para conseguir realizar o processo de desbloqueio para a realização de transações financeiras. Essas informações não são compartilhadas com terceiros.
3. Acessar fotos, mídias e arquivos do seu dispositivo. Necessário para criação dos comprovantes ao final da transação e selecionar foto na galeria para inclusão de foto de perfil. Nenhuma informação do seu celular é lida ou armazenada pela PREVCOM.

4.13. POLÍTCA DE COOKIES

Para oferecer a melhor experiência durante a navegação em nosso site e na internet, podemos usar cookies e coletar, tratar, armazenar e/ou compartilhar - entre a PREVCOM e outros parceiros - informações de sua navegação, para:

- garantir maior segurança durante a sua navegação;
- aperfeiçoar sua usabilidade, experiência e interatividade na utilização dos nossos portais, sites, aplicativos, e-mails e durante a sua navegação na internet;
- fazer ofertas e/ou te dar informações mais assertivas e relevantes às suas necessidades e interesses;
- buscar maior eficiência em relação à frequência e continuidade da nossa comunicação com você;
- responder suas dúvidas e solicitações;
- realizar pesquisas de comunicação e marketing de relacionamento, para melhorar nossos produtos e serviços, bem como apuração de estatísticas em geral.

A qualquer momento o usuário pode ativar em seu navegador mecanismos para informá-lo quando os mesmos estiverem acionados ou, ainda, para impedir que sejam.

O uso de cookies, arquivos criados pelos websites que, enquanto se navega na internet, são armazenados no navegador do usuário e ajudam a personalizar seu acesso, permite as seguintes vantagens:

- mais segurança durante a sua navegação;
- melhor usabilidade, experiência e interatividade na utilização dos nossos canais digitais;
- recebe informações e anúncios mais assertivos e relevantes às suas necessidades e interesses;
- participação em pesquisas de comunicação e marketing de relacionamento para melhorar nossos produtos e serviços.

Os cookies podem ser desativados por meio das preferências do navegador. A navegação pode se tornar limitada e algumas funcionalidades dos sites podem ficar comprometidas.

Caso a opção do usuário de configuração seja recusar cookies tal ferramenta será desabilitada durante a sua navegação. Caso o usuário aceite ou não configure seu navegador na forma como aqui descrito, entenderemos que você concordou com a execução de cookies conforme descrito nesta Política.

4.14. DESCRIÇÃO DOS COOKIES NO SITE DA PREVCOM

ASP.NET SESSION ID: Serviço de sessão do ASP.NET MVC (Linguagem de desenvolvimento do site) para identificação do usuário randômica, não utilizado pela PREVCOM, porém presente em todas as aplicações nesta linguagem.

GOOGLE ANALYTICS: Serviço de análise web fornecido pela Google, Inc. ("Google"). O Google Analytics utiliza uma forma específica de "Cookies", ou seja, arquivos de texto, que são armazenados no seu computador e permitem a análise do seu uso do site. A informação gerada pelo Cookie acerca da sua utilização do site será transmitida e armazenada em um servidor da Google nos EUA. A PREVCOM salienta que o Google Analytics foi ampliado no sítio eletrônico PREVCOM para incluir o código "gat._anonymizeIp ()." a fim de garantir a gravação anônima de endereços IP (as chamadas máscaras de IP). Devido à anonimização do IP neste site, o endereço IP do USUÁRIO/PARTICIPANTE é abreviado pela Google dentro do território da União Europeia e do Tratado da Comunidade Econômica Europeia. Só em casos excepcionais é que o endereço IP completo será transmitido a um servidor da Google nos EUA e aí então abreviado. A Google usa esta informação em nome da PREVCOM para analisar a utilização do USUÁRIOS do sítio eletrônico da PREVCOM, a fim de compilar relatórios sobre atividades do site e fornecer serviços adicionais relacionados ao seu uso e uso da Internet para o operador do site. O endereço IP transmitido para o Google Analytics pelo navegador do USUÁRIO/PARTICIPANTE não está consolidado com outros dados da Google. O USUÁRIO/PARTICIPANTE poderá impedir o armazenamento de Cookies por meio da definição adequada do software de navegação. Além disso, poderá impedir que a Google grave e processe os dados gerados pelos Cookies e relacionados ao uso do site (incluindo endereço IP), baixando e instalando o plug-in disponível no link e informações adicionais sobre os termos de uso e proteção de dados em https://www.google.com/analytics/terms/br.html ou https://www.google.com.br/intl/pt-BR/policies/privacy/.

TWITTER PLATAFORM: Serviço de análise web do Twitter com objetivo de otimizar o compartilhamento e acesso a plataforma Twitter por meio do site da PREVCOM.

COOKIES INTERNOS DE NAVEGAÇÃO: Utilizamos cookies de sessão em nossa área restrita a fim de tornar pessoal e otimizável o acesso a mesma. São cookies que guardam a preferência do usuário em relação ao modo padrão de exibição uma vez modificada.

4.15. DADOS PESSOAIS

A PREVCOM tem como uma de suas premissas a proteção dos dados pessoais de todas as pessoas envolvidas na sua cadeia de atividades. O direito à privacidade é uma prioridade e pauta todas as ações e políticas da PREVCOM. Dentre as atividades abrangidas por esta política, poderá ocorrer o Tratamento/Processamento de dados pessoais, ou seja, operações realizadas com dados pessoais, tais como, a coleta, produção, utilização, acesso, distribuição, processamento, arquivamento, eliminação, entre outros. Desta forma, qualquer Tratamento de dados realizado deverá respeitar as disposições gerais desta Política, além dos demais documentos corporativos e políticas aplicáveis ao tema.

4.16. EXCEÇÕES

Não se aplica.

4.17. REFERÊNCIAS

- Código de Ética de PREVCOM
- Política de Segurança da Informação da PREVCOM
- ISO/IEC 27701:2019
- Proteção de dados pessoais em conformidade com a Lei Brasileira 13.709/2018

5. TERMOS DE USO PARA SITES E APLICATIVOS

5.1. TERMOS DE USO

Estes Termos de Uso são aplicáveis a todos os sites e aplicativos da PREVCOM (inclusive sites e aplicativos institucionais, de produtos e serviços) e a todos que acessam os nossos serviços digitais.

Ao acessar nossos serviços, você expressamente aceita e concorda com as disposições destes Termos de Uso. Por conta disso, você deve ler atentamente esses termos antes de usar os nossos sites e aplicativos. Caso você não concorde com os Termos de Uso, você não deve usar os nossos sites e aplicativos.

5.2. ATUALIZAÇÃO DOS TERMOS DE USO

Lembramos que os Termos de Uso, assim como os conteúdos e funcionalidades dos nossos canais poderão ser atualizados a qualquer momento por razões legais, pelo uso de novas tecnologias e funcionalidades e sempre que a PREVCOM entender que as alterações são necessárias. **Ao continuar a acessar nossos sites e aplicativos após as alterações, que serão publicadas nos sites e aplicativos, você concorda com as alterações também.**

5.3. TERMOS E CONDIÇÕES DE USO ESPECÍFICOS

Além desses Termos de Uso e Política de Privacidade, alguns sites e aplicativos podem ter serviços e funcionalidades específicos e termos e condições adicionais para a sua utilização. Nesse caso, os termos adicionais estarão disponíveis em referidos sites e aplicativos e serão aplicáveis se você usar tais serviços e funcionalidades.

5.4. ACESSO A CONTEÚDO RESTRITO

Alguns dos nossos sites e aplicativos possuem área de conteúdo aberto e de conteúdo restrito. Para ter acesso ao conteúdo restrito, pode ser necessário que o usuário faça um cadastro fornecendo algumas informações pessoais para poder criar um login e senha.

Fique atento se as informações fornecidas estão corretas, pois você é responsável pela veracidade das mesmas, e caso tenha alguma inconsistência, pode impactar no seu acesso ao site ou aplicativo.

O usuário que se cadastrar no site utilizando dados de terceiros, poderá incorrer em prática de crimes, sem prejuízo de eventual responsabilização de acordo com a legislação.

5.5. CAPACIDADE PARA EFETUAR O CADASTRO

É proibido o cadastro de usuários que não tenham capacidade civil (com relação a pessoas físicas) ou não sejam representantes legais (com relação a pessoas jurídicas).

O usuário que se cadastrar no Site utilizando dados de terceiros, poderá incorrer em prática de crimes, sem prejuízo de eventual responsabilização de acordo com a legislação.

5.6. COMO MEUS DADOS DE CADASTRO SÃO UTILIZADOS?

A PREVCOM coleta informações durante o processo de cadastro para a gestão do Site, administração, prestação, ampliação e melhoria dos produtos ofertados e dos serviços prestados. Você pode conferir os dados pessoais coletados e como são usados pela Fundação. Para mais esclarecimento ou consultas use o e-mail privacidade.prevcom@sp.gov.br.

5.7. POSSO COMPARTILHAR MEU LOGIN E SENHA E COM TERCEIROS?

Somente você pode utilizar o seu login e senha, sendo assim proibido o compartilhamento com terceiros. Note que o seu acesso é pessoal e intransferível, e você é inteiramente responsável pela guarda, sigilo e bom uso do seu login e senha.

5.8. CONTEÚDOS ENVIADOS POR USUÁRIOS

Alguns de nossos sites e aplicativos podem permitir que os usuários enviem conteúdos como comentários, imagens, mensagens, fotos etc., para divulgação em áreas de conteúdo aberto dos sites e aplicativos. Para estes casos, os conteúdos enviados e a identificação do seu perfil, se houver, poderão ser visualizados por outros usuários, atendendo sempre as normas e regulamentações específicas.

Pode também ser possível ao usuário enviar conteúdo, como fotos, documentos, comentários e outras mensagens para fins de cadastro, atendimento, para uso de serviços disponíveis nos sites e aplicativos ou outras finalidades. Nesses casos, os conteúdos enviados não ficarão disponíveis em áreas de conteúdo aberto dos sites e aplicativos.

Lembramos que, em qualquer dos casos, os conteúdos enviados serão de responsabilidade única e exclusiva de quem os enviou.

A PREVCOM reserva-se o direito de reprovar, restringir ou eliminar comentários em desacordo com o propósito de avaliação de Produtos, ou que ofendam a honra, imagem, reputação e/ou dignidade de terceiros.

5.9. ENVIO DE COMUNICAÇÕES PELO APLICATIVO

Para te manter informado sobre sua conta, produtos e serviços da PREVCOM, além de informações sobre segurança, poderemos te mandar mensagens pelo aplicativo do celular (*push*). Caso não queira receber notificações em seu celular, você poderá desabilitar o recebimento nas configurações do seu sistema operacional. Se tivermos uma informação muito importante para lhe passar, enviaremos a mensagem mesmo com a permissão desabilitada.

5.10. LINKS PARA SITES E APLICATIVOS DE TERCEIROS

Nossos sites e aplicativos podem conter links para sites e aplicativos de terceiros. Note que dentro destes sites e aplicativos de terceiros você estará sujeito a outros termos de uso e políticas de privacidade. Nossos Termos de Uso e Política de Privacidade não são válidos nos sites e aplicativos de terceiros. A existência desses links não significa nenhuma relação de endosso ou de patrocínio entre a PREVCOM e esses terceiros, e a PREVCOM não tem nenhuma responsabilidade com relação a tais terceiros.

5.11. COMO NOSSOS SITES E APLICATIVOS NÃO DEVEM SER UTILIZADOS

Fique atento às seguintes práticas que vão contra as nossas condições de uso:

- Praticar qualquer ato ilícito, violar direitos da PREVCOM ou de terceiros e violar a legislação vigente.
- Upload, envio ou transmissão de qualquer conteúdo erótico, pornográfico, obsceno, calunioso, difamatório, de violência física ou moral, com apologia ao crime, uso de drogas, consumo de bebidas alcoólicas ou produtos para fumo, bem como que promova ou incite o ódio, atividades ilegais, o preconceito ou qualquer outra forma de discriminação por qualquer motivo.
- Usar qualquer sistema/aplicação automatizada para realizar consultas, acessos ou qualquer outra operação massificada, para qualquer finalidade, sem autorização da PREVCOM.
- Praticar atos que prejudiquem qualquer site, aplicativo e equipamento da PREVCOM e de outros usuários e terceiros, seja por meio de vírus, trojans, malware, worm, bot, backdoor, spyware, rootkit, ou qualquer outro meio com este fim.

5.12. RESPONSABILIDADES

Você como usuário é responsável:

- por todas as suas ações ou omissões realizadas nos nossos sites e aplicativos.
- pelos conteúdos que você enviou e/ou transmitiu nos sites e aplicativos. e
- pela reparação de danos causados a PREVCOM, terceiros ou outros usuários, a partir do seu acesso e uso dos nossos sites e aplicativos.

Desta forma, não nos responsabilizamos pelos itens citados acima e por indisponibilidades e falhas técnicas do sistema dos sites e aplicativos. Considere também que conteúdos enviados e/ou transmitidos por usuários e/ou terceiros não representam a opinião ou a visão da PREVCOM.

5.13. PROPRIEDADE INTELECTUAL

Os seguintes itens pertencem a PREVCOM e somente podem ser usados com sua prévia e expressa autorização:

- todos os softwares, aplicativos ou funcionalidades criadas, produzidos ou contratados pela PREVCOM para os sites e aplicativos, assim como sua identidade visual e conteúdo.
- os nomes das empresas, marcas, patentes, nomes de domínio, slogans, propagandas ou qualquer sinal utilizado para distinguir o que é da PREVCOM inseridos nos sites e aplicativos.

No caso de conteúdos que você enviar ou transmitir pelos sites e aplicativos, você autoriza a PREVCOM a utilizar os direitos intelectuais sobre eles em caráter irrevogável, sem qualquer restrição ou limitação de qualquer natureza.

A utilização pela PREVCOM destes conteúdos enviados por você observará o previsto neste dispositivo. Você também garante que os conteúdos por você enviados não infringem direitos de terceiros.

Ao acessar o Site o usuário declara que irá respeitar todos os direitos de propriedade intelectual e industrial, os decorrentes da proteção de marcas registradas, bem como todos os direitos referentes a terceiros que porventura estejam ou estiveram, de alguma forma, disponíveis no Site. O simples acesso ao Site não confere ao usuário qualquer direito ao uso dos nomes, títulos, marcas, patentes, obras literárias, artísticas, imagens, modelos entre outras, que nele estejam ou estiveram disponíveis.

5.14. SUSPENSÃO DE ACESSO

A qualquer momento, sem aviso prévio ou posterior, a PREVCOM poderá suspender, cancelar ou interromper o acesso aos sites e aplicativos, inclusive se o uso destes canais contrariar o disposto neste documento.

5.15. ENTRE EM CONTATO CONOSCO

Se você tem dúvidas sobre estes Termos e Condições de Uso ou sobre o nosso Site em geral, por favor entre contato pelo e-mail: privacidade.prevcom@sp.gov.br.

5.16. DADOS PESSOAIS

A PREVCOM tem como uma de suas premissas a proteção dos dados pessoais de todas as pessoas envolvidas na sua cadeia de atividades. O direito à privacidade é uma prioridade e pauta todas as ações e políticas da PREVCOM. Dentre as atividades abrangidas por esta política, poderá ocorrer o Tratamento/Processamento de dados pessoais, ou seja, operações realizadas com dados pessoais, tais como, a coleta, produção, utilização, acesso, distribuição, processamento, arquivamento, eliminação, entre outros. Desta forma, qualquer Tratamento de dados realizado deverá respeitar as disposições gerais desta Política, além dos demais documentos corporativos e políticas aplicáveis ao tema.

5.17. LEGISLAÇÃO APLICÁVEL

A legislação brasileira é aplicável a estes Termos de Uso e Política de Privacidade. O usuário deste Site se submete ao Foro da Cidade de São Paulo/SP, com exceção de qualquer outro.

6. POLÍTICA PARA MANUSEIO DE DADOS PESSOAIS

6.1. OBJETIVO

A presente Política para Manuseio de Dados Pessoais ("Política") tem como objetivo determinar as regras internas para o manuseio de dados pessoais.

Para os fins do presente Política, deve-se entender por manuseio de dados pessoais:

- Toda a operação de tratamento de dados pessoais, como, por exemplo, a coleta, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, atualização, comunicação, transferência, compartilhamento e extração.

6.2. RESPONSABILIDADES

- Diretoria.
- Gerência de Tecnologia da Informação – TI.
- Todos os colaboradores envolvidos com o tema.

6.3. DEFINIÇÕES

- **Anonimização:** Processo pelo qual um dado relativo ao titular não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.
- **Colaboradores**: São todos os empregados da PREVCOM, incluindo conselheiros e diretores.
- **dados pessoais:** Qualquer informação relativa a uma pessoa singular identificada ou identificável. é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como - por exemplo - um nome, um número de identificação, dados de localização, identificadores por via eletrônica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, econômica, cultural ou social dessa pessoa singular.
- **Encarregado de Dados:** Pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de dados (ANPD).
- **Relatório de Impacto à proteção de dados pessoais:** Documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.
- **Titular:** Pessoa física a quem se referem os dados pessoais.
- **Terceiros**: São todos os prestadores de serviços, trabalhadores terceirizados, parceiros comerciais e fornecedores com quem a PREVCOM compartilha dados pessoais

6.4. REGISTRO DAS OPERAÇÕES DE TRATAMENTO DE DADOS PESSOAIS

Todas as operações de tratamento de dados pessoais devem ser registradas em documento específico para tal fim, que contenha, no mínimo:

a) A área responsável pelo tratamento;

b) A finalidade do tratamento;

c) Quais dados pessoais são tratados;

d) De quem são os dados pessoais tratados (cliente, corretor, fornecedor, colaboradores etc.);

e) Se há o tratamento de dados pessoais de crianças;

f) Se há o compartilhamento desses dados com terceiros (inclusive transferência internacional);

g) Base legal autorizadora do tratamento.

É obrigação do Encarregado de Dados pela proteção de dados pessoais manter o registro das atividades de tratamento de dados pessoais atualizado.

Sempre que julgar necessário, o Encarregado de Dados poderá solicitar informações adicionais à área responsável pelo tratamento dos dados pessoais, especialmente, para a realização de monitoramento e fiscalização.

6.5. REGRAS GERAIS PARA O TRATAMENTO DE DADOS PESSOAIS

Em toda e qualquer operação de tratamento de dados pessoais, sejam eles obtidos diretamente do titular, de terceiros ou de bases públicas, deverão ser observadas as seguintes regras:

- **Finalidade**: O manuseio de dados pessoais deverá ser realizado unicamente para o cumprimento de uma finalidade específica, pré-determinada e informada ao titular.
- **Necessidade:** O manuseio deverá ser restrito ao mínimo de dados pessoais necessário para o alcance da finalidade pré-definida.
- **Não Discriminação:** O manuseio de dados pessoais não poderá ser realizado para fins discriminatórios ilícitos.
- **Qualidade**: A PREVCOM deverá se atentar para a precisão, qualidade e acurácia dos dados que manuseia.
- **Transparência:** Deverá ser garantida a transparência ao titular sobre o tratamento de seus dados pessoais.

6.6. COMPARTILHAMENTO DE DADOS PESSOAIS

Ao compartilhar dados pessoais com terceiros, (enviar ou receber dados), deverão ser observadas as regras estabelecidas na Política de Compartilhamento de Dados Pessoais, a Política de Privacidade de Dados e a Política de Privacidade de Dados de Colaboradores.

6.7. ARMAZENAMENTO DE DADOS PESSOAIS

Os documentos que contenham dados pessoais não poderão ser armazenados por período superior ao necessário para o cumprimento da finalidade pretendida, independentemente do formato utilizado, se físico ou eletrônico.

6.8. DADOS PESSOAIS SENSÍVEIS

No manuseio de dados pessoais sensíveis, deverão ser observadas as hipóteses autorizadoras específicas para tanto. São dados pessoais sensíveis aquelas relativas à:

- Origem racial ou étnica;
- Convicção religiosa;
- Opinião política;
- Filiação a sindicato;
- Organização de carácter religioso, filosófico ou político;
- Saúde ou à vida sexual; e
- Dado genético ou biométrico.

No caso de dúvidas sobre a classificação de qualquer dado pessoal como sensível, o Encarregado de Dados deverá ser consultado.

6.9. DADOS PESSOAIS DE CRIANÇAS

O manuseio de dados pessoais de crianças, deverá ser realizado:

- Em seu melhor interesse, ou seja, com a finalidade de beneficiá-las, ainda que de forma indireta;
- Com transparência, considerando as condições físico-motoras, perceptivas, sensoriais, intelectuais e mentais dos destinatários, com o uso de recursos audiovisuais, quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança.

O tratamento de dados pessoais de crianças necessitará da prévia coleta do consentimento expresso, específico e em destaque, de pelo menos um dos pais ou responsáveis legais.

Exceções deverão ser aprovadas pelo Encarregado de Dados.

6.10. HIPÓTESES AUTORIZADORAS PARA O TRATAMENTO DE DADOS PESSOAIS

Para que uma atividade de tratamento de dados pessoais possa ser realizada, ela deve ser fundamentada em uma das hipóteses autorizadoras (bases legais) abaixo:

6.10.1. CUMPRIMENTO DE OBRIGAÇÃO LEGAL OU REGULATÓRIA

Existência de lei, norma, decisão judicial ou regulação vigente, pela qual o tratamento se torna obrigatório (e não opcional). Exemplos:

- Arquivamento de notas fiscais;
- Manutenção de documentos conforme exigências do Banco Central, SUSEP, CVM e B3;
- Controle de ponto de colaboradores;
- Envio de dados ao e-Social.

6.10.2. EXECUÇÃO DE CONTRATO OU PROCEDIMENTOS PRELIMINARES AO CONTRATO

Quando necessário o tratamento para a execução de contrato ou de procedimentos preliminares relacionados a um contrato, do qual o titular seja parte. Exemplos:

- Entrega de produtos e prestação de serviços aos clientes;
- Atendimento a clientes;
- Recrutamento e seleção;
- Pagamento de colaboradores;
- Fornecimento de benefícios aos colaboradores.

6.10.3. EXERCÍCIO REGULAR DE DIREITO

Para o exercício regular de direitos em processo judicial, administrativo ou arbitral, em trâmite ou futuro. Exemplos:

- Arquivo de processos judiciais;
- Arquivo de documentos para defesa em processos trabalhistas;
- Procurações para atuação em processos judiciais ou administrativos;
- Documentos de comprovação para obtenção de benefícios fiscais;

Para o tratamento de dados sensíveis, a legislação prevê que o exercício regular de direito também será aplicável no âmbito contratual.

6.10.4. TUTELA DA SAÚDE

Para garantir a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária, sendo vedado qualquer outro uso que desvirtue essa finalidade. Exemplos:

- Procedimentos de Medicina do Trabalho;
- Exames laboratoriais.

6.10.5. PROTEÇÃO DA VIDA OU INCOLUMIDADE FÍSICA

Para garantir a proteção da vida ou incolumidade física do titular ou de terceiros, quando em iminente perigo. Exemplo, em atendimentos médicos de emergência.

6.10.6. PROTEÇÃO AO CRÉDITO

Para garantir a proteção ao crédito, observando-se a legislação vigente (como: Lei do Cadastro Positivo e Código de Defesa do Consumidor). Exemplos:

- Consultas a cadastros para concessão de crédito;
- Manutenção de histórico de adimplementos para futuras concessões de crédito.

6.10.7. PREVENÇÃO À FRAUDE E À SEGURANÇA DO TITULAR

Para prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos. Exemplos:

- Fechaduras/catracas biométricas;
- Reconhecimento facial em cadastros de acesso, com a finalidade de garantir a segurança;

Essa base legal se encontra prevista exclusivamente para as hipóteses de tratamento de dados pessoais sensíveis.

6.10.8. LEGÍTIMO INTERESSE

Para garantir a continuidade da atividade econômica/operação dos agentes de tratamento, desde que o titular dos dados tenha expectativa quanto à atividade de tratamento. Exemplos:

- Estudos e relatórios internos sobre as atividades da Fundação;
- Avaliações de desempenho de Colaboradores;
- Oferta de serviços adicionais a titulares que já são clientes (Participantes);
- Auditorias internas.

É importante destacar que o tratamento de dados pessoais com base em interesses legítimos não será permitido, caso ameace ou lesione direitos e liberdades fundamentais do titular.

Quando o tratamento for realizado com base no legítimo interesse, o Encarregado de Dados poderá elaborar Relatório de Impacto à Proteção de Dados Pessoais, quando necessário.

6.10.9. CONSENTIMENTO

Pode ser utilizado para fundamentar qualquer atividade de tratamento, desde que seja livre, expresso, informado e inequívoco. Contudo, o tratamento realizado com base unicamente no consentimento fica restrito à vontade do titular, que pode, a qualquer tempo, revogá-lo.

Nos casos em que a base legal adequada para o tratamento seja o consentimento, deverá ser observado a Política de Uso e Gestão do Consentimento.

6.11. RESPONSABILIDADES

Compete ao Encarregado de Dados:

- Analisar e aprovar ou reprovar as solicitações de suspensão de prazo de armazenamento de dados pessoais;
- Analisar situações em que os dados pessoais de crianças poderão ser manuseados sem o consentimento expresso de um dos pais ou responsável legal;
- Elaborar Relatório de Impacto à Proteção de Dados Pessoais, quando necessário;
- Manter o registro das operações de manuseio de dados pessoais, contemplando a respectiva base legal.

Compete à Área responsável pelo manuseio de dados pessoais

- Observar e atender as regras definidas nesta Política, quando aplicáveis.

6.12. PENALIDADES

O cumprimento de todas as Políticas publicadas é exigido de todos os Colaboradores da PREVCOM, constituindo-se em violação a não observância aos preceitos nelas descritos, podendo acarretar na aplicação de medidas disciplinares, tais como advertência verbal, escrita ou até mesmo em desligamento por justa causa, dependendo da gravidade da falta cometida.

6.13. DADOS PESSOAIS

A PREVCOM tem como uma de suas premissas a proteção dos dados pessoais de todas as pessoas envolvidas na sua cadeia de atividades. O direito à privacidade é uma prioridade e pauta todas as ações e políticas da PREVCOM. Dentre as atividades abrangidas por esta política, poderá ocorrer o Tratamento/Processamento de dados pessoais, ou seja, operações realizadas com dados pessoais, tais como, a coleta, produção, utilização, acesso, distribuição, processamento, arquivamento, eliminação, entre outros. Desta forma, qualquer Tratamento de dados realizado deverá respeitar as disposições gerais desta Política, além dos demais documentos corporativos e políticas aplicáveis ao tema.

6.14. CONSIDERAÇÕES FINAIS

Para o esclarecimento de dúvidas, entre em contato com o Encarregado pelo Tratamento de dados pessoais da Fundação pelo e-mail: privacidade.prevcom@sp.gov.br.

O cumprimento deste Procedimento é de suma importância e dever de todos. Em caso de não observância deste procedimento, favor reportar imediatamente ao Encarregado pela Proteção de Dados, pelo e-mail: privacidade.prevcom@sp.gov.br.

As denúncias de violações às Políticas e Procedimentos serão anônimas e a não-retaliação será garantida.

6.15. DOCUMENTOS RELACIONADOS

Normativos internos relacionados ao tema, não se limitando a:

- Política para Uso e Gestão do Consentimento.
- Regimento Interno do Comitê de Privacidade e Proteção de dados pessoais.
- Código de Conduta.
- Norma de Transparência no Tratamento de dados pessoais.
- Política de organização de trabalhos orientados a privacidade de dados.
- Política de Privacidade
- Política de Privacidade de Colaboradores

6.16. EXCEÇÕES

Não se aplica.

7. POLÍTICA DE COMPARTILHAMENTO DE DADOS PESSOAIS COM TERCEIROS

7.1. OBJETIVO

O objetivo do presente documento é determinar as regras aplicáveis ao compartilhamento de dados pessoais que sejam de conhecimento da PREVCOM com terceiros.

Para esse fim considera-se compartilhamento de dados com terceiros toda a comunicação, difusão, transferência (inclusive internacional), interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados.

Exemplos:

- Armazenamento destes dados em serviços de *cloud*;
- Transferência de dados pessoais para empresas parceiras, a fim de executar serviços contratados por um titular;
- Envio de relação de colaboradores para fornecedores de benefícios.

O compartilhamento de dados pessoais com terceiros somente poderá ser realizado para o atendimento da finalidade previamente informada ao titular de forma que garanta a transparência do tratamento.

É responsabilidade do gestor da área que realiza o compartilhamento garantir que estas determinações sejam devidamente cumpridas.

7.2. RESPONSABILIDADES

- Diretoria.
- Gerência de Tecnologia da Informação – TI.
- Todos os colaboradores envolvidos com o tema.

7.3. DEFINIÇÕES

- **Agentes de Tratamento**: O Controlador e o Operador de dados pessoais.
- **Anonimização:** Processo pelo qual um dado relativo ao titular não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.
- **Comitê de Privacidade:** Grupo de pessoas, composto pelo Encarregado, responsável por tomar as decisões relativas a projetos classificados com alto nível de sensibilidade.
- **Encarregado:** Pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de dados (ANPD).
- **dados pessoais:** Qualquer informação relativa a uma pessoa singular identificada ou identificável. É considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em

especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrônica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, econômica, cultural ou social dessa pessoa.

- **Dados Pessoais Sensíveis:** Qualquer dado pessoal que diga respeito à origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou à organização de caráter religioso, filosófico ou político, bem como dado referente à saúde ou à vida sexual, dado genético ou biométrico.
- **Pseudonimização:** É o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional, mantida separada pelo controlador em ambiente controlado e seguro.
- **Terceiro:** São todos os prestadores de serviços, trabalhadores terceirizados, parceiros comerciais, fornecedores e representantes da PREVCOM.
- **Titular dos dados pessoais:** Pessoa natural a quem se referem os dados pessoais objeto de compartilhamento pela PREVCOM.
- **Relatório de Impacto:** Documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.
- **Gestor da Área:** Pessoa designada pela PREVCOM para gerir uma determinada área dentro da sua estrutura.
- **Uso Compartilhado De Dados:** Comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados.
- **Colaboradores:** São todos os empregados da PREVCOM, incluindo conselheiros e diretores.
- **Terceiros:** São todos os prestadores de serviços, trabalhadores terceirizados, parceiros comerciais e fornecedores com quem a PREVCOM compartilha dados pessoais

7.4. CENÁRIOS DE COMPARTILHAMENTO

O Compartilhamento de dados pessoais com terceiros deverá ser classificado de acordo com o grau de exposição do dado pessoal. Esta classificação deverá ser realizada pelo próprio Gestor da Área Solicitante/Responsável pelo compartilhamento, com o auxílio do Encarregado de Dados, quando necessário. A escala a seguir se propõe a orientar essa classificação.

Grau de Exposição	Quem pode autorizar o compartilhamento	Descrição do grau de exposição do dado pessoal
Muito baixo	Gestor da área ou responsável pelo compartilhamento	Quando há compartilhamento de dados pessoais Anonimizados ou estatísticos que não possibilitam a identificação de um titular de Dados.
Baixo	Encarregado	Quando um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro.
Médio	Encarregado e diretoria envolvida	Quando há o compartilhamento de dados pessoais sem qualquer procedimento para mascaramento ou vínculo direto com o titular.
Alto	Subcomissão de Privacidade e diretoria envolvida	Quando há compartilhamento de dados pessoais classificados como: (i) dados pessoais Sensíveis. (ii) dados pessoais de criança e adolescente. (iii) dados pessoais Financeiros. (iv) dados pessoais de Comportamento.
Muito alto	Subcomissão de Privacidade e Diretoria Executiva	Quando há compartilhamento/transferência internacional de dados pessoais.

7.5. REGRAS GERAIS PARA TODAS AS ATIVIDADES DE COMPARTILHAMENTO DE DADOS PESSOAIS

Em regra, toda a atividade que envolva o compartilhamento de dados pessoais deverá ser embasada em contrato ou aditivo contratual.

A Subcomissão de Segurança e Privacidade, em linha com a área jurídica da PREVCOM deverá assegurar, quando pertinente, que os contratos contemplem cláusulas que resguardem os direitos dos titulares e os interesses da PREVCOM, relativos à privacidade e proteção de dados pessoais.

Sempre que julgar necessário, o Encarregado poderá solicitar a realização de auditoria para garantir que o terceiro está observando todas as regras previstas em contrato.

Caso, não seja possível a formalização de um contrato ou aditivo contratual, o compartilhamento de dados deverá, obrigatoriamente, ser aprovado pelo Subcomissão de Segurança e Privacidade e por uma diretoria da PREVCOM (por exemplo, envio de dados pessoais para o INSS).

7.6. RELATÓRIO DE AVALIAÇÃO

Sempre que for necessário compartilhar dados pessoais, o gestor da área solicitante pelo compartilhamento, deverá gerar um relatório com as seguintes informações:

a) O propósito/objetivo do compartilhamento;

b) Os dados que a PREVCOM precisa compartilhar para atingir a finalidade pretendida;

c) Indicar se é possível atingir a finalidade indicada, sem o Compartilhamento dos dados pessoais, ou mediante sua respectiva Anonimização;

d) Indicar o que aconteceria se o dado pessoal não fosse compartilhado;

e) A existência de alguma proibição legal para o compartilhamento dos dados pessoais pela PREVCOM;

f) Quais os riscos identificados em realizar o compartilhamento, considerando as diligências descritas no item "DILIGÊNCIAS" desta política; e

g) Quando e como os dados pessoais devem ser compartilhados.

Estas informações compõe o Relatório de Avaliação que será a base para a aprovação do compartilhamento.

Conforme o grau de exposição da informação, este relatório será encaminhado para um público específico. O Encarregado pela proteção dos dados é o responsável pela condução e organização desse processo de aprovação e liberação.

7.7. LIMITAÇÕES AO COMPARTILHAMENTO

Em toda a atividade de compartilhamento de dados pessoais, deverão ser observadas as seguintes limitações:

- **Compartilhamento de dados pessoais sensíveis de saúde**: dados pessoais que se referem à saúde do indivíduo não podem ser compartilhados com terceiros com finalidade de se obter vantagem econômica e
- **Compartilhamento de dados pessoais de Crianças**: dados pessoais de crianças (até 12 anos) somente poderá ser compartilhado com terceiros mediante consentimento expresso dos pais ou responsável (eis).

7.8. DILIGÊNCIAS

O Departamento responsável pelo compartilhamento deverá, previamente ao compartilhamento, avaliar se o terceiro:

- Observa as normas relativas à privacidade e proteção de dados pessoais;
- Possui um programa de privacidade e proteção de dados pessoais;
- Adota as medidas necessárias para garantir a segurança dos dados pessoais que manuseia;
- Possui um plano de resposta a incidentes relativo a dados pessoais;
- Já sofreu algum tipo de incidente e/ou autuação relativos ao tratamento de dados pessoais.

O Encarregado de Dados deverá monitorar o cumprimento das obrigações relativas à privacidade e proteção de dados pessoais, pelos Terceiros, durante a vigência do contrato e/ou da operação de compartilhamento.

7.9. RESPONSABILIDADES

Compete ao Encarregado de Dados:

a) Aprovar o Relatório descrito no item "RELATÓRIO DE AVALIAÇÃO" desta política, emitido pelo Gestor da Área Solicitante/Responsável pelo compartilhamento, nos casos de operações com níveis de exposição baixo e médio.

b) Emitir o parecer a respeito do Relatório descrito no item "RELATÓRIO DE AVALIAÇÃO desta Política, e submetê-lo à aprovação da subcomissão de Segurança e Privacidade, nos casos de operações com níveis de exposição alto e muito alto.

c) Realizar o acompanhamento periódico/monitoramento das operações de compartilhamento, tomando as medidas necessárias para mitigar eventuais riscos identificados.

d) Nas operações de compartilhamento de sensibilidade crítica, assegurar-se que:

   a. o grau de proteção de dados pessoais do país destinatário tenha sido reconhecido pela ANPD como adequado ao previsto na legislação brasileira vigente. e

   b. o terceiro destinatário garanta o cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados adotado pela legislação brasileira vigente.

e) Manter o registro das operações de Compartilhamento com terceiros, contemplando a respectiva base legal e elaborar o Relatório de Impacto à Proteção de Dados Pessoais, quando entender necessário.

f) Garantir que as diligências prévias e necessárias ao compartilhamento de dados pessoais tenham sido observadas pela área responsável pelo compartilhamento.

g) Armazenar o registro relativo às diligências para o compartilhamento de dados pessoais, realizadas pela Área responsável pelo compartilhamento.

Compete à área responsável pelo compartilhamento:

- Observar e atender as diretrizes definidas nesta política, quando aplicáveis.
- Realizar e documentar as diligências prévias e necessárias ao compartilhamento de dados pessoais com terceiros, com o intuito de comprovar a adequação dos seus procedimentos frente a auditorias, testes de controle, fiscalizações, entre outras situações.
- Emitir o relatório de avaliação descrito nesta política, e submetê-lo ao Encarregado para aprovação ou emissão de parecer.

Compete a Assessoria Jurídica e a Subcomissão de Segurança e Privacidade:

- Observar os requerimentos regulatórios locais e os padrões de cláusulas contratuais da Fundação, quando da redação ou revisão das cláusulas dos contratos firmados com terceiros.
- Assegurar, quando pertinente, que os contratos contemplem cláusulas que resguardem os direitos dos titulares e os interesses da Fundação, relativos à privacidade e proteção de dados pessoais.

7.10. PENALIDADES

O cumprimento de todas as Políticas e procedimentos publicados é exigido de todos os colaboradores da PREVCOM, constituindo-se em violação a não observância aos preceitos nelas descritos, podendo acarretar a aplicação de medidas disciplinares, tais como advertência verbal, escrita ou até mesmo em desligamento por justa causa, dependendo da gravidade da falta cometida.

7.11. CONSIDERAÇÕES FINAIS

Para o esclarecimento de dúvidas, entre em contato pelo e-mail: privacidade.prevcom@sp.gov.br.

Em caso de não observância desta política, favor reportar imediatamente ao Encarregado pelo Tratamento de dados pessoais, pelo e-mail: privacidade.prevcom@sp.gov.br

As denúncias de violações às Políticas e procedimentos serão anônimas e a não-retaliação será garantida.

7.12. DADOS PESSOAIS

A PREVCOM tem como uma de suas premissas a proteção dos dados pessoais de todas as pessoas envolvidas na sua cadeia de atividades. O direito à privacidade é uma prioridade e pauta todas as ações e políticas da PREVCOM. Dentre as atividades abrangidas por esta política, poderá ocorrer o Tratamento/Processamento de dados pessoais, ou seja, operações realizadas com dados pessoais, tais como, a coleta, produção, utilização, acesso, distribuição, processamento, arquivamento, eliminação, entre outros. Desta forma, qualquer tratamento de dados realizado deverá respeitar as disposições gerais desta Política, além dos demais documentos corporativos e políticas aplicáveis ao tema.

7.13. EXCEÇÕES

Não se aplica.

7.14. DOCUMENTOS RELACIONADOS

Normativos internos relacionados ao tema, não se limitando a:

- Política de Manuseio de dados pessoais.
- Política para Uso e Gestão do Consentimento.
- Regimento Interno da Comissão de Privacidade e Segurança da Informação.
- Código de Conduta.
- Política de organização de trabalhos orientados a privacidade de dados
- Política de Privacidade
- Política de Privacidade de dados de Colaboradores

8. POLÍTICA DE USO E GESTÃO DO CONSENTIMENTO

8.1. OBJETIVO

A presente Política para Uso e Gestão de Consentimento no Tratamento de dados pessoais tem por objetivo determinar as regras aplicáveis ao uso do consentimento como base legal para o tratamento de dados pessoais, devendo ser observada por todos os Colaboradores da PREVCOM.

8.2. RESPONSABILIDADES

- Diretoria.
- Gerência de Tecnologia da Informação – TI.
- Todos os colaboradores envolvidos com o tema.

8.3. DEFINIÇÕES

Anonimização: Processo pelo qual um dado relativo ao titular não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.

Colaboradores: São todos os empregados da PREVCOM, incluindo conselheiros e diretores.

Consentimento: Autorização livre, específica, informada e inequívoca concedida pelo titular para o tratamento de seus dados pessoais.

dados pessoais: Qualquer informação relativa a uma pessoa singular identificada ou identificável. é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como - por exemplo - um nome, um número de identificação, dados de localização, identificadores por via eletrônica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, econômica, cultural ou social dessa pessoa singular.

Encarregado: Pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de dados (ANPD).

Titular: Pessoa física a quem se referem os dados pessoais.

Terceiros: São todos os prestadores de serviços, trabalhadores terceirizados, parceiros comerciais e fornecedores com quem a PREVCOM compartilha dados pessoais.

8.4. ORIENTAÇÕES GERAIS

O consentimento é uma manifestação do titular do Dado Pessoal que autoriza o tratamento de seus dados pessoais. Para o consentimento ser válido, deve-se:

- Obedecer a uma finalidade (objetivo) específica, não genérica. Esta finalidade deve ser apresentada ao titular do Dado Pessoal de maneira clara e antes da coleta do consentimento. (Por exemplo, “Ao clicar no quadrado abaixo, você autoriza o uso de seu nome e e-mail para envio de e-mails personalizados com anúncios de parceiros”).
- Garantir que se deu de forma livre e inequívoca.

- Destacá-lo das demais disposições e contratuais. e
- Preferencialmente, apresentá-lo de forma granular.

Seguem mais considerações sobre termos aplicados ao consentimento:

- **Consentimento livre:** O consentimento livre pressupõe que o titular não tenha sido compelido a autorizar o tratamento dos seus dados. Assim, essa base legal somente será apropriada se, ao titular, for oferecida uma escolha genuína em relação a aceitar ou recusar os termos oferecidos para o tratamento dos seus dados.
- **Consentimento informado:** Fácil e de imediato acesso às informações sobre como os dados do titular serão tratados, os efeitos do fornecimento e discordância da autorização solicitada. A linguagem utilizada deve ser clara e de fácil entendimento para o público-alvo. Recomenda-se a adoção de mensagens curtas e diretas. O titular deve ser, no mínimo, informado sobre: (i) a finalidade de cada uma das operações de tratamento em relação às quais se procura obter o consentimento. (ii) quais dados serão coletados e utilizados.
- **Consentimento inequívoco:** para que o consentimento seja inequívoco, é preciso que este seja dado por meio de uma ação positiva do titular, ou seja, tem de ser óbvio que o titular dos dados deu o consentimento para o tratamento de seus dados pessoais. Exemplo: utilização de caixas pré-selecionadas ou utilização de cookies dos usuários que não deram aceites nos avisos externos. Para o consentimento ser inequívoco é necessário que o titular tenha uma ação afirmativa para concedê-lo, como marcar o checkbox ou clicar no item de aceite de cookies etc. O responsável pelo tratamento deve se atentar para o fato de que o consentimento não pode ser obtido por meio da mesma ação de concordar com o contrato ou aceitar as condições gerais do serviço (comumente chamadas de "Li e Concordo"). A aceitação de condições gerais não pode ser confundida com o ato inequívoco de consentir com o tratamento dos dados pessoais.
- **Finalidade específica e determinada:** Os dados não poderão ser tratados para uma finalidade distinta daquela consentida pelo titular. Nesse contexto, para que a PREVCOM obtenha o consentimento válido, deverá garantir ao titular máxima transparência sobre a finalidade para a qual pretende tratar os seus dados pessoais. Caso a PREVCOM tenha a intenção de tratar os dados para outra finalidade deverá obter novo consentimento para a nova finalidade ou certificar-se da existência uma outra base legal que permita este tratamento.

8.5. FORNECIMENTO DE INFORMAÇÕES E OBTENÇÃO DO CONSENTIMENTO

A área responsável pela coleta do consentimento deverá adaptar a linguagem e design/layout das informações e da requisição de consentimento, conforme o seu destinatário e os meios empregados para o registro dos dados e da obtenção do consentimento (meio telefônico, formulários web, contratos, formulários em suporte físico, entre outros).

Em qualquer caso, as áreas da PREVCOM que tratem dados pessoais com base no consentimento, deverão usar as cláusulas/scripts de informação e requisição do consentimento, previamente aprovados pelo Encarregado pela Proteção de Dados Pessoais designado pela Fundação. Se o consentimento for solicitado como parte de contrato, o responsável pela área jurídica da Fundação deve assegurar que este seja requerido de maneira destacada ou em documento apartado.

8.6. CONSENTIMENTO PARA O TRATAMENTO DE DADOS PESSOAIS SENSÍVEIS

Dados pessoais sensíveis são informações que versam sobre a origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de carácter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico de um indivíduo.

Quando utilizado para tratar dados sensíveis, além de observar as demais regras previstas nesta Política, o consentimento deve:

- Se dar de forma específica, ou seja, direcionada exclusivamente para o tratamento de tais informações;
- Ser inserido de maneira destacada dos demais termos e requisições de autorização/contrato.

8.7. CONSENTIMENTO PARA O TRATAMENTO DE DADOS DE CRIANÇAS

Em decorrência da vulnerabilidade de indivíduos menores de 12 (doze) anos de idade, o tratamento de seus dados pessoais deverá ocorrer apenas em hipóteses excepcionais e mediante a coleta do consentimento específico e em destaque, fornecido por pelo menos um dos pais ou pelo responsável legal do indivíduo. Este consentimento poderá ser em folha apartada ou em campo especial e em destaque no documento principal.

Ao coletar o consentimento de um dos pais ou responsável legal pela criança, a área que efetivar o tratamento destes dados deverá exigir comprovação do vínculo legal existente entre a criança e aquele que se declara responsável legal e manter as evidências desta verificação.

8.8. O ÔNUS DA PROVA QUANTO AOS REQUISITOS DO CONSENTIMENTO VÁLIDO

É da PREVCOM a responsabilidade de demonstrar que todos os requisitos necessários para a validade do consentimento foram devidamente observados, no momento da obtenção do consentimento junto ao titular dos dados.

Dessa forma, é necessário que o responsável da área que manuseia dados pessoais com base no consentimento adeque as informações e a requisição do consentimento ao canal pelo qual o procedimento tenha sido realizado (telefone, online ou presencial), e mantenha integral registro da operação.

Para esses fins, recomenda-se a gravação de chamadas telefônicas, manutenção de cópias dos documentos assinados pelos titulares dos dados, bem como registros eletrônicos gerados pelas plataformas por meio das quais os procedimentos tenham ocorrido.

É de responsabilidade do Encarregado garantir que essas informações sejam armazenadas e documentadas de forma organizada.

8.9. OPOSIÇÃO E REVOGAÇÃO DO CONSENTIMENTO

Deverá ser garantido ao titular dos dados pessoais a revogação facilitada e de forma gratuita do seu consentimento, quando este assim desejar. Na coleta do consentimento, a área responsável pelo tratamento dos dados pessoais deverá informar o meio para revogação, bem como garantir meios seguros e facilitados para que o titular possa revogar esta autorização, sem a necessidade de se apresentar qualquer justificativa.

Caso os dados pessoais tenham sido compartilhados com Terceiros, a Área responsável pelo compartilhamento reportará a revogação do consentimento pelo titular ao departamento jurídico, que deverá notificar esses Terceiros

comunicando o ocorrido e requisitando a interrupção do tratamento dos dados pessoais, caso não haja outra base legal que autorize este tratamento.

O Encarregado pela Proteção de dados pessoais será responsável por monitorar se as solicitações de revogação estão sendo devidamente respondidas e observadas pelos Terceiros.

8.10. GESTÃO DO CONSENTIMENTO

Para gerir o consentimento de forma eficiente, o Encarregado pela Proteção de dados pessoais deve garantir a constante atualização do registro de atividades de tratamento e respectivas bases legais. Dessa forma, quando um titular de dados pessoais revogar o consentimento, a PREVCOM será capaz de identificar a atividade à qual o titular se refere e responder à sua solicitação de forma assertiva e em prazo razoável.

O Encarregado deverá também:

- Revisar periodicamente a atividade de tratamento baseada em consentimento, para garantir que não houve mudança na finalidade para a qual o titular deu seu consentimento;
- Garantir que dados pessoais dos titulares que revogaram seu consentimento não sejam tratados sem que haja outra base legal que autorize o tratamento; e
- Garantir que a Fundação disponibilize método simplificado para que o titular possa, a qualquer momento, revogar o consentimento ou exercer quaisquer direitos do titular estabelecidos na Lei Geral de Proteção de Dados.

8.11. RESPONSABILIDADES

Compete ao Encarregado de Dados:

- Garantir a constante atualização do registro de atividades de tratamento e respectivas bases legais;
- Monitorar periodicamente a atividade de tratamento baseada em consentimento, para garantir que não houve mudança na finalidade para a qual o titular deu seu consentimento;
- Garantir que dados pessoais dos titulares que revogaram seu consentimento não sejam tratados sem que haja outra base legal que autorize o tratamento;
- Garantir que a Fundação disponibilize método simplificado e gratuito para que o titular possa, a qualquer momento, revogar o consentimento ou exercer quaisquer direitos do titular estabelecidos na Lei Geral de Proteção de Dados;
- Aprovar as cláusulas/scripts de informação e requisição do consentimento;
- É de responsabilidade do Encarregado garantir que os registros relativos à obtenção e revogação do consentimento sejam armazenados e documentados de forma organizada; e
- Monitorar se as solicitações de revogação estão sendo devidamente respondidas e observadas pelos Terceiros.

Compete à área que realiza a atividade de tratamento cuja base legal seja o consentimento:

- Observar e atender as diretrizes definidas nesta Política, quando aplicáveis;

- Adaptar a linguagem e design/layout das informações e da requisição de consentimento, conforme o seu destinatário e os meios empregados para o registro dos dados e da obtenção do consentimento (meio telefônico, formulários web, contratos, formulários em suporte físico, entre outros);
- Utilizar as cláusulas/scripts de informação e requisição do consentimento, previamente aprovados pelo Encarregado;
- Exigir comprovação do vínculo legal entre a criança e aquele que se declara responsável legal e manter as evidências desta verificação, quando obtiver o consentimento para o tratamento de dados pessoais de crianças; e
- Informar ao titular, o meio para a revogação do consentimento, bem como garantir meios seguros e facilitados para que o titular possa revogar esta autorização, sem a necessidade de se apresentar qualquer justificativa.

Compete ao Departamento Jurídico:

- Assegurar, quando pertinente, que os contratos contemplem cláusulas destacadas ou apartadas para a obtenção do consentimento.

8.12. DADOS PESSOAIS

A PREVCOM tem como uma de suas premissas a proteção dos dados pessoais de todas as pessoas envolvidas na sua cadeia de atividades. O direito à privacidade é uma prioridade e pauta todas as ações e políticas da PREVCOM. Dentre as atividades abrangidas por esta política, poderá ocorrer o Tratamento/Processamento de dados pessoais, ou seja, operações realizadas com dados pessoais, tais como, a coleta, produção, utilização, acesso, distribuição, processamento, arquivamento, eliminação, entre outros. Desta forma, qualquer tratamento de dados realizado deverá respeitar as disposições gerais desta Política, além dos demais documentos corporativos e políticas aplicáveis ao tema.

8.13. PENALIDADES

O cumprimento de todas as Políticas publicadas é exigido de todos os Colaboradores da PREVCOM, constituindo-se em violação a não observância aos preceitos nelas descritos, podendo acarretar a aplicação de medidas disciplinares, tais como advertência verbal, escrita ou até mesmo em desligamento por justa causa, dependendo da gravidade da falta cometida.

8.14. CONSIDERAÇÕES FINAIS

Para o esclarecimento de dúvidas, entre em contato pelo canal privacidade.prevcom@sp.gov.br

O cumprimento desta Política é de suma importância e dever de todos. Em caso de não observância desta Política, favor reportar imediatamente ao Encarregado pela Proteção de Dados, pelo e-mail: privacidade.prevcom@sp.gov.br

As denúncias de violações às Políticas e Procedimento serão anônimas e a não-retaliação será garantida.

8.15. EXCEÇÕES

Não se aplica.

8.16. DOCUMENTOS RELACIONADOS

Normativos internos relacionados ao tema, não se limitando a:

- Política de Manuseio de dados pessoais.
- Política para Uso e Gestão do Consentimento.
- Regimento Interno do Comitê de Privacidade e Proteção de dados pessoais.
- Código de Conduta.
- Norma para Garantir a Transparência ao titular.
- Política de organização de trabalhos orientados a privacidade de dados.
- Política de Privacidade
- Política de Privacidade de Colaboradores

9. GLOSSÁRIO

AGENTES DE TRATAMENTO: O Controlador e o Operador de dados pessoais.

ANONIMIZAÇÃO: Processo pelo qual um dado relativo ao Titular não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.

APROVADOR: Pessoa formalmente autorizada pelo gestor da informação para aprovação da concessão de acessos.

ÁREAS CUSTODIANTES: Áreas delegadas pelos gestores das informações "I/O - Information Owners" que, por definição da Fundação, tem autonomia em relação ao ciclo de vida de aquisição, desenvolvimento e manutenção dos sistemas.

ARTEFATOS CORPORATIVOS: Produtos, serviços, processos, práticas de negócio ou sistemas.

ATIVO DE INFORMAÇÃO: Toda informação, não importando a mídia que a suporte e que represente valor para os negócios da Fundação de Previdência Complementar do Estado de São Paulo.

AUTENTICIDADE: Propriedade da informação que confirma a originalidade de seu conteúdo, comprovando sua origem e sua autoria.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS ("ANPD"): Órgão pertencente à administração pública federal, responsável pela fiscalização do cumprimento das disposições da Lei Geral de Proteção de Dados.

BYOD (BRING YOUR OWN DEVICE): Conceito que permite o uso de dispositivos móveis pessoais para exercer suas atividades no ambiente de trabalho conforme normas e requisitos estabelecidos pela Fundação.

CLASSIFICAÇÃO DE DADOS: A Política de Classificação Eletrônica de Risco de Sistema e dados tem o objetivo de descrever a confidencialidade dos dados em questão e não leva em consideração os requisitos de integridade ou disponibilidade em sua classificação. A classificação dos dados pode depender do contexto em que os dados são usados.

CLOUD COMPUTING: Computação (sistemas, banco de dados, aplicação, etc.) em nuvem, ou seja, é a entrega de serviços de TI onde o acesso é possível por meio de qualquer dispositivo, estando dentro ou fora da rede da Fundação e empregando a internet como meio de comunicação.

COLABORADOR (ES): São todos os empregados e funcionários da PREVCOM, incluindo conselheiros e diretores.

COMITÊ DE PRIVACIDADE: Grupo de pessoas, composto pelo Encarregado, responsável por tomar as decisões relativas a Projetos classificados com alto Nível de Sensibilidade.

CONFIDENCIALIDADE: Propriedade da informação que garante que o conteúdo é acessível somente por pessoas autorizadas.

CONFLITO DE INTERESSES: Situações nas quais a atuação do funcionário ou Fornecedor indica a busca de quaisquer vantagens e/ou benefícios próprios ou de terceiros, em detrimento dos interesses da Fundação.

CONSENTIMENTO: Manifestação livre, informada e inequívoca do titular que autoriza o tratamento dos seus dados pessoais para uma finalidade específica.

CONTAS / LOGIN: Identificação de um usuário na rede corporativa, aplicativos ou outros recursos de processamento de informações.

CONTROLADOR: Parte que determina as finalidades e os meios de Tratamento de dados pessoais.

COORDENAÇÃO DE INFRA E SUPORTE: É o responsável técnico, da área de TI, pelo ambiente de sistemas, aplicações, suporte técnico e componentes de TI da Fundação.

COORDENAÇÃO DE SEGURANÇA E PRIVACIDADE: É o responsável, técnico da área de TI, por processos de segurança da informação e privacidade de dados da Fundação.

DADOS ANONIMIZADOS: dados objeto de utilização de meios técnicos razoáveis e disponíveis no momento do Tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo.

DADOS COMPORTAMENTAIS: dados pessoais que demonstrem ou revelem o comportamento do Titular. Exemplos: dados de localização, consumo, hábitos, preferências, endereço IP, cookies, logs de conexão, logs de acesso.

DADOS FINANCEIROS: dados pessoais que remetam ou revelem qualquer aspecto financeiro do titular. Exemplos: número de conta, cartão de crédito, senha, código verificador, renda, salário, benefícios.

DADOS PESSOAIS SENSÍVEIS: dados pessoais sobre origem racial, étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, referente à saúde, ou à vida sexual, Dado genético ou biométrico, quando vinculados a uma pessoa natural.

DADOS PESSOAIS: Quaisquer informações relativas a uma pessoa singular identificada ou identificável. é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrônica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, econômica, cultural ou social dessa pessoa singular.

DAR: Documento de Aceitação de Riscos, utilizado para formalizar os riscos de determinado projeto ou situação.

DISPONIBILIDADE: Propriedade da informação que garante que usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

ENCARREGADO: Pessoa indicada pelo Controlador e operador para atuar como canal de comunicação entre o Controlador, os titulares dos dados e a Autoridade Nacional de Proteção de dados (ANPD).

FINALIDADE: Motivo pelo qual o dado pessoal será tratado, ou objetivo que se pretende atingir com o tratamento dos dados.

FORNECEDOR: Toda pessoa física ou jurídica, pública ou privada, nacional ou estrangeira, bem como os entes despersonalizados, que desenvolvem atividades de produção, montagem, criação, construção, transformação, importação, exportação, distribuição ou comercialização de produtos ou prestação de serviços à Fundação, necessários e utilizados na execução do objeto social da Fundação.

FRAUDE: é qualquer ato ardiloso, enganoso, de má-fé com o intuito de lesar ou ludibriar outrem, ou de não cumprir determinado dever, obtendo para si ou outrem vantagem ou benefícios indevidos (pecuniários ou não). Subterfúgio para alcançar um fim ilícito e/ou engano dolosamente provocado, induzimento ao erro ou aproveitamento de preexistente erro alheio.

GESTOR DA ÁREA: Pessoa designada pela PREVCOM para gerir uma determinada área dentro da sua estrutura.

GESTOR DA INFORMAÇÃO ("INFORMATION OWNERS"): Diretores ou níveis hierárquicos acima, responsáveis pelas informações geradas e/ou manuseadas para realização dos processos de negócio da Fundação de Previdência Complementar do Estado de São Paulo.

GESTOR DE ACESSOS: Pessoa formalmente nomeada para apoio na implementação das regras de aprovação e concessão de acessos.

GESTOR DO PROJETO: Colaborador designado pela PREVCOM para gerir um Projeto e que será responsável pela resposta do Questionário de Avaliação de Sensibilidade.

HIGIENIZAÇÃO: Processo pelo qual os dados (informações, registros) são removidos irreversivelmente do dispositivo ou destruídos permanentemente.

INCIDENTE DE SEGURANÇA DE INFORMAÇÕES: Qualquer evento que afete ou possa afetar, de forma prejudicial e/ou maliciosa, os negócios e/ou a integridade física e/ou lógica dos ambientes da Fundação de Previdência Complementar do Estado de São Paulo.

INCIDENTES: Acesso, aquisição, uso, compartilhamento, destruição, alteração ou indisponibilidade de dados pessoais, proposital ou acidental, não autorizada ou ilícita. Violação da confidencialidade, integridade e disponibilidade de dados pessoais. Exemplos: Perda de laptop com dados pessoais de colaboradores, que não estejam criptografados. Envio de e-mail que contenha dados pessoais de clientes, para o destinatário errado. Arquivo de currículos de candidatos a uma vaga exposto em um diretório aberto na internet, com acesso sem necessidade de identificação (usuário e senha). Extração de dados pessoais de servidores da Fundação por um terceiro que utilize de falhas técnicas e engenharia social ("ataque hacker").

INFORMAÇÕES CORPORATIVAS: Informações direta ou indiretamente envolvidas na operação dos sistemas corporativos da Fundação de Previdência Complementar do Estado de São Paulo, independentemente do local onde tenham sido produzidas.

INFORMATION OWNER: Responsável (gestor) das informações de um sistema ou módulo do sistema.

INTEGRIDADE: Propriedade da informação que garante a salvaguarda da exatidão e completude da informação.

LEGALIDADE: Propriedade que garante que a informação se encontra em concordância com as legislações vigentes e aplicáveis a Fundação de Previdência Complementar do Estado de São Paulo.

LIMPEZA / SUBSTITUIÇÃO BINÁRIA: o software grava zeros, uns e depois um pseudoaleatório sobre os dados existentes.

MATERIAIS, BENS E SERVIÇOS: Qualquer bem, móvel ou imóvel, material ou imaterial, assim como qualquer atividade fornecida mediante remuneração, que são adquiridos pela PREVCOM.

MESA LIMPA: Prática na qual, ao final do expediente, os documentos considerados confidenciais ou uso interno são armazenados em locais seguros, tais como: armário e gavetas disponíveis com chaves.

NÃO REPÚDIO: Propriedade da informação em que o autor não pode negar a responsabilidade sobre ele atribuída. Consegue-se estabelecer a característica de não repúdio com a combinação de confidencialidade e integridade da informação.

NOME DE USUÁRIO (USERNAME): é a chave única de identificação do usuário para acesso à rede, correio eletrônico e sistemas, também conhecido como login.

OWASP (OPEN WEB APPLICATION SECURITY PROJECT): Entidade dedicada a capacitar organizações para conceber, desenvolver, adquirir, operar e manter aplicações que precisam ser confiáveis para desenvolvimento de aplicações *web*.

PERFIL DE ACESSO: Conjunto de permissões definidas em um sistema ou aplicativo focado nas necessidades de um determinado posto de trabalho ou cargo seguindo as necessidades do negócio.

PROJETO: Toda e qualquer atividade e/ou iniciativa para concepção, desenvolvimento e/ou atualização de novos produtos ou serviços de interesse da PREVCOM.

PROPRIETÁRIO DA INFORMAÇÃO: é o colaborador responsável por gerenciar, garantir a segurança e o uso adequado das informações sob sua responsabilidade.

PSEUDONIMIZAÇÃO: É o Tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional, mantida separada pelo Controlador em ambiente controlado e seguro.

QUESTIONÁRIO DE AVALIAÇÃO DE RISCO: Documento com perguntas elaboradas e estruturadas para extrair respostas que revelem informações relacionadas às operações de Tratamento de dados pessoais no Projeto, de modo a permitir a avaliação e classificação do Nível de Risco. Objeto do Anexo I.

QUESTIONÁRIO DE LEGÍTIMO INTERESSE ("LIA"): Documento com perguntas elaboradas e estruturadas para extrair respostas que revelem informações relacionadas à utilização do Legítimo Interesse como base legal de Tratamento de dados pessoais no Projeto. Objeto do Anexo II.

RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS: Documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.

REQUISITANTE: Responsável por emitir a requisição de compras necessária para solicitar a contratação de um material ou serviço.

SEGREGAÇÃO DE FUNÇÕES: Princípio básico de controle que consiste na separação de funções, normalmente de autorização, aprovação, execução e controle, de tal forma que nenhuma pessoa, pelo acúmulo de privilégios, detenha competências em desacordo com este princípio.

SEGURANÇA DA INFORMAÇÃO: Conjunto de medidas que visam a preservação da confidencialidade, integridade, autenticidade, legalidade e disponibilidade das informações.

SEGURANÇA FÍSICA E PATRIMONIAL: Conjunto de medidas que têm por objetivo a proteção contra ocorrências, visando evitar, conter e/ou minimizar atos deliberados que possam ou não causar danos às pessoas, ao patrimônio, às informações, à execução dos serviços ou à imagem da Fundação de Previdência Complementar do Estado de São Paulo.

SENHA FORTE: Conjunto de caracteres recomendados que, quando da verificação da identidade de um usuário, gera maior segurança e proteção contra *hackers, softwares* maliciosos etc..

SISTEMA DE CONTROLE DE ACESSO: Sistema de controle que garante que os acessos sejam efetuados apenas por pessoas autorizadas.

SISTEMA DE INFORMAÇÃO: Conjunto de informações relacionadas, de modo a formar uma base de conhecimento sobre um processo, suportada ou não por programas de computador.

SYSTEM OWNER DE INFRA/APLICAÇÃO: Responsável técnico pelo funcionamento do sistema/aplicação.

TERCEIROS: São todos os prestadores de serviços, trabalhadores terceirizados, parceiros comerciais, fornecedores e representantes da PREVCOM.

TESTES DE SEGURANÇA: Testes a serem aplicados aos sistemas de informação visando à validação sobre o atendimento dos requerimentos de segurança.

TITULAR DOS DADOS: Pessoa natural a quem se referem os dados pessoais objeto de Tratamento pela PREVCOM.

TRATAMENTO: Qualquer operação ou conjunto de operações efetuadas com dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a coleta, o registro, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, a eliminação ou a destruição

USERNAME: Chave única de identificação do usuário para acesso à rede, correio eletrônico e sistemas também conhecido como *login*.

USO COMPARTILHADO DE DADOS: Comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento

de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados.

USUÁRIO DA INFORMAÇÃO: Pessoa que tem como papel, utilizar-se das informações da Fundação de Previdência Complementar do Estado de São Paulo no desempenho de suas atividades e em conformidade com a política e normas de segurança da informação.