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.