

Título: BIBLIOTECA DE POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE DE DADOS PESSOAIS				
Emitido por:	COMISSÃO CONSULTIVA DE MUDANÇAS, SEGURANÇA E PRIVACIDADE	Código Instrumento V-001	Revisão 03	Data de Emissão 01/12/2020

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.

Título: BIBLIOTECA DE POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE DE DADOS PESSOAIS				
Emitido por:	COMISSÃO CONSULTIVA DE MUDANÇAS, SEGURANÇA E PRIVACIDADE	Código Instrumento V-001	Revisão 03	Data de Emissão 01/12/2020

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.

Título: BIBLIOTECA DE POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE DE DADOS PESSOAIS				
Emitido por:	COMISSÃO CONSULTIVA DE MUDANÇAS, SEGURANÇA E PRIVACIDADE	Código Instrumento V-001	Revisão 03	Data de Emissão 01/12/2020

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.

Título: BIBLIOTECA DE POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE DE DADOS PESSOAIS				
Emitido por:	COMISSÃO CONSULTIVA DE MUDANÇAS, SEGURANÇA E PRIVACIDADE	Código Instrumento V-001	Revisão 03	Data de Emissão 01/12/2020

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

Emitido por:	COMISSÃO CONSULTIVA DE MUDANÇAS, SEGURANÇA E PRIVACIDADE	Código Instrumento V-001	Revisão 03	Data de Emissão 01/12/2020
--------------	--	-----------------------------	---------------	-------------------------------

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.