Política de Segurança da Informação

Estruturação de Governança em Segurança da Informação

Aprovada pelo Conselho Deliberativo da Entidade
na reunião de 26 de junho de 2026

SUMÁRIO

EMBRAER PREV – Sociedade de Previdência Complementar
Rua Euclides Miragaia, 145, Sala 1404 – Centro – CEP 12.245-820 – São José dos Campos - SP
Telefone: (12) 3307 7091

1. OBJETIVO

O objetivo deste documento é definir regras e boas práticas para acesso e utilização a todos os sistemas, equipamentos, instalações e informações com base nos requisitos comerciais e de segurança para obtenção de acesso.

Estabelecer as diretrizes para criação, transmissão, processamento, utilização, armazenamento, recuperação e descarte de informações a fim de preservar as informações quanto aos seguintes princípios:

- **Confidencialidade:** garantia de que o acesso à informação esteja disponível somente para pessoas, entidades ou processos autorizados;
- **Integridade:** garantia de que a informação seja mantida em seu estado original, exata e completa;
- **Disponibilidade:** garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

A **EMBRAER PREV** considera em suas políticas de segurança da informação o processo contínuo no qual os riscos são identificados, analisados, avaliados, tratados e reduzidos a um nível aceitável.

2. REFERÊNCIA

- NBR ISO IEC 27001: 2022
- NBR ISO IEC 27002: 2022

3. RESPONSABILIDADES

Este documento aplica-se a todo o escopo do Sistema de Gestão da Segurança da Informação (SGSI), isto é, a todos os sistemas, equipamentos, instalações, recursos humanos e informações do escopo do SGSI da **EMBRAER PREV.** Os procedimentos com Provedores Externos (Parceiros e Prestadores de serviços), envolvidos com processos da **EMBRAER PREV**, serão tratados no Capítulo 18 desta Política.

3.1. Colaborador

3.1.1. É da responsabilidade de cada colaborador da **EMBRAER PREV**, o prejuízo ou dano que vier a sofrer ou causar a **EMBRAER PREV** ou a terceiros em decorrência da não obediência às diretrizes desta política.

3.1.2. Notificar os incidentes, fragilidades ou ainda, suspeitas de fragilidades de segurança da informação observadas na **EMBRAER PREV**.

EMBRAER PREV – Sociedade de Previdência Complementar
Rua Euclides Miragaia, 145, Sala 1404 – Centro – CEP 12.245-820 – São José dos Campos - SP
Telefone: (12) 3307 7091

3.2. Gestor das Unidades Organizacionais

3.2.1. Incentivar e monitorar o cumprimento da política de segurança da informação pelos colaboradores sob sua gestão.

3.2.2. Garantir a adaptação aos processos, procedimentos e aos sistemas sob sua responsabilidade para que atendam à política de segurança da informação.

3.2.3. Definir direitos e níveis de acesso de todos os colaboradores sob sua gerência.

3.2.4. Realizar análise crítica e periódica das permissões de acesso juntamente com o departamento de TI da **EMBRAER PREV**.

3.2.5. Definir níveis de segurança para todas as informações que fazem parte do seu processo e promover a rotulagem de acordo com a política de classificação e tratamento da informação.

3.2.6. Identificar os riscos associados aos ativos da informação pertinentes ao seu processo e realizar a análise crítica periódica dos riscos associados a esses ativos.

3.3. Departamento de RH

3.3.1. Atribuir aos colaboradores, durante a formalização da contratação a responsabilidade pelo cumprimento da política de segurança da informação.

3.3.2. Após o processo de contratação do colaborador, independente do regime de contrato, apresentar essa política e demais normativos internos solicitar a assinatura tanto dela, quanto do Termo de Confidencialidade e dos demais normativos.

3.3.3. Comunicar e divulgar a política de segurança da informação a todos os colaboradores, recomendando as medidas que forem cabíveis, como treinamentos periódicos e eventos de conscientização.

3.3.4. Aplicar as sanções previstas na política de segurança quando for o caso.

3.4. Departamento de TI

3.4.1. Monitorar e auditar o ambiente tecnológico, através da implantação de sistema de monitoramento dos servidores, e-mails, conexões com a internet, dispositivos móveis ou wi-fi e todos outros componentes de rede.

3.4.2. Configurar todos os equipamentos e ferramentas concedidos aos colaboradores com todos os controles necessários para cumprir os requisitos de segurança da informação estabelecidos nesta política.

EMBRAER PREV – Sociedade de Previdência Complementar
Rua Euclides Miragaia, 145, Sala 1404 – Centro – CEP 12.245-820 – São José dos Campos - SP
Telefone: (12) 3307 7091

3.4.3. Segregar as funções administrativas e operacionais a fim de restringir ao mínimo necessário os privilégios de cada indivíduo e reduzir a existência de colaboradores que possam excluir os logs e trilhas de auditoria das suas próprias ações.

3.4.4. Analisar e criar todos os acessos aos sistemas que são pertinentes ao trabalho dos colaboradores, após solicitação do coordenador/gerente ou sócio responsável.

3.5. Aquisição, Desenvolvimento e Manutenção de Sistemas

3.5.1 Analisar e criar todos os acessos às ferramentas de desenvolvimento de sistemas.

3.5.2. Garantir que sistemas são desenvolvidos seguindo os princípios de segurança estabelecidos nesta política.

3.6. Segurança da Informação e Processos

3.6.1. O Departamento constitui um grupo de trabalho para tratar de questões, propor soluções, metodologias e processos específicos de segurança da informação.

3.6.2. É responsável pela análise das infrações cometidas pelos colaboradores frente a esta política, com consequência de incidente, devendo examinar a gravidade e riscos sob o enfoque técnico e legal de cada infração cometida, resultando na recomendação de processo disciplinar para apuração dos fatos e aplicação das ações disciplinares cabíveis, para eventual e futuro encaminhamento às autoridades policiais ou judiciais, quando necessário.

4. OBRIGAÇÕES E PERMISSÕES DOS USUÁRIOS

4.1. Toda conta de acesso é atribuída a um único usuário e será de sua responsabilidade o uso para fins estritamente relacionados ao desempenho de suas atividades dentro do escritório, não podendo permitir ou colaborar com o acesso aos recursos computacionais por parte de pessoas não autorizadas e nem compartilhar com outros usuários de forma alguma.

4.2. O perfil de acesso dos usuários aos aplicativos e sistemas poderá ser usado somente para o desempenho de suas atividades na **EMBRAER PREV**.

4.3. O usuário será responsável pela segurança de sua conta de acesso e senha, pelas informações armazenadas nos equipamentos dos quais faz uso e por qualquer atividade neles desenvolvida.

4.4. O RH deve informar ao departamento de TI, quando todos os acessos de um determinado colaborador se tornam desnecessários.

EMBRAER PREV – Sociedade de Previdência Complementar
Rua Euclides Miragaia, 145, Sala 1404 – Centro – CEP 12.245-820 – São José dos Campos - SP
Telefone: (12) 3307 7091

4.5. O acesso à informação e às funções dos sistemas de aplicação devem ser restringidos por meio de controle dos direitos de acesso dos colaboradores de forma a limitar quais dados ou funções dos sistemas de aplicação poderão ser acessados por determinado colaborador e qual o nível de permissão.

5. POLÍTICA DE SENHAS DE ACESSO

A fim de zelar pela integridade e confidencialidade de suas credenciais e dos dados do escritório e efetivamente contribuir para a efetiva gestão do controle de acesso aos sistemas, e arquivos o usuário deve seguir as seguintes regras:

5.1. Manter a confidencialidade de sua senha, ou seja, a sua senha é pessoal e intransferível, não deverá ser repassada para ninguém, em hipótese alguma.

5.2. Assim que conectar a primeira vez e que utilizar sua conta de acesso aos sistemas, essa senha deverá ser alterada de acordo com a especificação abaixo.

5.3. Criar senhas que sejam fáceis de lembrar, mas que não sejam baseadas em elementos que outras pessoas ou possíveis invasores possam facilmente adivinhar, ou deduzir, a partir de informações pessoais, como, por exemplo:

- Nome do usuário.
- Identificador do usuário (ID), mesmo que seus caracteres estejam embaralhados.
- Nome de membros da sua família ou de amigos íntimos.
- Nomes de pessoas ou lugares em geral.
- Nome do sistema operacional ou da máquina que está sendo utilizada.
- Datas significativas, como a do nascimento próprio, de um filho, esposa, etc.
- Números de telefone, de cartão de crédito, de carteira de identidade ou de outros documentos pessoais.
- Placas ou marcas de veículos.
- Palavras que constam de dicionários em qualquer idioma.
- Letras ou números repetidos.

5.4. Solicitar uma nova senha, quando do esquecimento.

5.5. Evitar o registro das senhas em qualquer meio.

5.6. Alterar a senha sempre que existir qualquer indicação de possível comprometimento de sua confidencialidade.

5.7. Em caso de troca de senhas, evitar a reutilização de senhas antigas.

5.8. Escolher suas próprias senhas.

EMBRAER PREV – Sociedade de Previdência Complementar
Rua Euclides Miragaia, 145, Sala 1404 – Centro – CEP 12.245-820 – São José dos Campos - SP
Telefone: (12) 3307 7091

5.9. Selecionar senhas de boa qualidade, evitando o uso de senhas muito curtas ou muito longas, que o obrigue a registrá-las em qualquer outro meio para não serem esquecidas.

- É recomendável que a senha deve respeitar os critérios de complexidade abaixo:
  - Para usuários comuns, possuir 8 caracteres e, para usuário com privilégio administrativo, conter 14 caracteres;
  - Uma ou mais letras minúsculas;
  - Pelo menos 1 letra maiúscula;
  - Pelo menos 1 caractere numérico;
  - Pelo menos 1 caractere especial (! @, #, $, %, %, &, ,*).

5.10. Encerrar as sessões ativas ou utilizar-se do mecanismo de bloqueio de acesso (tela de proteção com senha) quando precisar se afastar dos equipamentos, mesmo que seja por um período curto.

5.11. Não revelar credenciais de acesso ou permitir o acesso a ativos de informação por terceiros por meio dessas credenciais.

5.12 Deve-se evitar a transferência de senhas e sempre que se fizer necessário enviar uma senha para outro colaborador, esta deve ser anotada em sistema web de compartilhamento de notas confidenciais de uso único.

6. CLASSIFICAÇÃO DAS INFORMAÇÕES

6.1. A definição do grau de sensibilidade das informações sensíveis deve possibilitar:

6.1.2. A determinação das salvaguardas mínimas para proteger as informações;

6.1.3. Garantir a continuidade operacional de utilização destas informações;

6.2. Informações documentadas devem ser identificadas, armazenadas, transmitidas e descartadas de acordo com um processo formal.

6.3. A classificação da informação é de responsabilidade do gestor da Unidade Organizacional onde a informação tem origem.

6.4. Toda rotulagem da informação é de responsabilidade do dono do processo em que a informação tem origem, com a finalidade de proteger os registros conforme requisitos legais, regulamentares, contratuais e do negócio.

6.5. O grau de sensibilidade da informação deve ser avaliado quanto à necessidade de proteger a CID - Confidencialidade, Integridade, Disponibilidade - da informação.

EMBRAER PREV – Sociedade de Previdência Complementar
Rua Euclides Miragaia, 145, Sala 1404 – Centro – CEP 12.245-820 – São José dos Campos - SP
Telefone: (12) 3307 7091

6.6. O grau de criticidade da operação se refere às consequências causadas pela interrupção das capacidades de processamento de informações, ou seja, quando afeta a disponibilidade

6.7 – Nível de confidencialidade

NÍVEL DE CONFIDENCIALIDADE	RÓTULOS	CRITÉRIOS DE CLASSIFICAÇÃO	RESTRIÇÃO DE ACESSO
Público (Site da **EMBRAER PREV**)	Sem rótulo	São informações públicas podem não prejudicar a **EMBRAER PREV**.	Disponíveis a todos.
Uso interno (Sistema, Diretórios de rede, documentos, processos)	Interno ou sem rótulo	São informações que podem causar pequenos danos e/ou inconveniências a **EMBRAER PREV**, quando são acessadas sem a devida autorização.	Somente os colaboradores da **EMBRAER PREV** e terceiros devidamente autorizados.
Confidencial (Senhas, Dados pessoais dos colaboradores e participantes)	Confidencial	Pode ocasionar danos irreparáveis a **EMBRAER PREV**, caso pessoas não autorizadas tenham acesso.	Disponibilizada somente para colaboradores na **EMBRAER PREV**

7. POLÍTICA PARA USO DOS ATIVOS

7.1. A **EMBRAER PREV** disponibiliza para seus colaboradores equipamentos exclusivamente para o desempenho de suas atividades profissionais, portanto, o uso inadequado desses equipamentos e para fins que não sejam os delineados pela **EMBRAER PREV**, está totalmente proibido.

7.2. O colaborador deve zelar pelo bom uso dos recursos de informática a ele disponibilizados não removendo, alterando ou acrescentando, qualquer tipo de componente interno de *hardware* ou *software*.

7.3. É vedado o armazenamento, na rede da **EMBRAER PREV** ou em quaisquer equipamentos de propriedade da **EMBRAER PREV**, material obsceno, ilegal ou não ético, fato que ensejará a apuração de responsabilidade.

EMBRAER PREV – Sociedade de Previdência Complementar
Rua Euclides Miragaia, 145, Sala 1404 – Centro – CEP 12.245-820 – São José dos Campos - SP
Telefone: (12) 3307 7091

7.4. Arquivos particulares ou não pertinentes ao negócio da **EMBRAER PREV** não devem ser copiados/movidos para a rede da **EMBRAER PREV,** pois podem sobrecarregar o armazenamento nos servidores. Caso seja identificada a existência desses arquivos, eles serão excluídos definitivamente sem aviso prévio.

7.5. Arquivos particulares ou não pertinentes ao negócio da **EMBRAER PREV** não devem ser armazenados nos dispositivos disponibilizados pela **EMBRAER PREV.**

7.6. Documentos necessários para as atividades da **EMBRAER PREV** devem ser salvos na rede. Tais arquivos, se gravados apenas nas estações de trabalho, poderão ser perdidos caso ocorra alguma falha no computador.

7.7. O colaborador não deve consumir alimentos e bebidas muito próximo aos recursos tecnológicos e aos documentos físicos corporativos, podendo ser responsabilizado por danos causados em decorrência deste ato.

7.8. O colaborador não deve alterar nenhuma configuração do equipamento, previamente configurado pelo departamento de TI.

7.9. É proibida a conexão de quaisquer equipamentos que não sejam de propriedade da **EMBRAER PREV** ou homologados pela **EMBRAER PREV**, em sua rede corporativa, especialmente os *notebooks* e *smartphones* particulares, já que comprometem a segurança da informação e a qualidade dos serviços.

8. POLÍTICAS DE MESA E TELA LIMPAS

8.1. As mesas de trabalho devem estar limpas de papéis e mídias de armazenamento removíveis que contenham informações sensíveis.

8.2. Os papéis e mídias contendo informações sensíveis devem ser guardados em local seguro, imediatamente após a utilização.

8.3. As áreas de trabalho dos computadores devem estar limpas de arquivos que contenham informações sensíveis. Estes arquivos terão que ser armazenados e utilizados diretamente na rede.

8.4. Sempre que for se ausentar da frente do computador, deverá ser feito o bloqueio do mesmo.

EMBRAER PREV – Sociedade de Previdência Complementar
Rua Euclides Miragaia, 145, Sala 1404 – Centro – CEP 12.245-820 – São José dos Campos - SP
Telefone: (12) 3307 7091

9. POLÍTICA PARA USO DE DISPOSITIVOS MÓVEIS E TRABALHO REMOTO

9.1. É responsabilidade do colaborador, no caso de furto ou roubo de um dispositivo móvel oferecido pela **EMBRAER PREV,** notificar o departamento de RH, para que o departamento de TI faça a alteração de todas as senhas, procurar ajuda das autoridades policiais registrando, assim que possível, um boletim de ocorrência.

9.2. O colaborador está ciente de que o uso indevido do dispositivo móvel caracterizará a assunção de todos os riscos da sua má utilização, sendo o responsável por quaisquer danos, diretos ou indiretos, presentes ou futuros, que venha causar à **EMBRAER PREV** ou a terceiros.

9.3. O trabalho remoto à rede da organização será feito via One Drive e Sharepoint da Microsoft, e a solicitação será feita pelo gerente/coordenador, que pode dar permissão somente às pastas pertencentes à equipe que ele gerencia/coordena.

9.4. É proibido pela **EMBRAER PREV** a utilização de mídias removíveis como pen drive e HD externo.

9.5. As informações da **EMBRAER PREV**, não devem ser acessadas, armazenadas ou processadas de qualquer maneira via dispositivos móveis pessoais. Dispositivos móveis pessoais podem ser utilizados para facilitar a comunicação entre membros da **EMBRAER PREV**, desde que nenhuma informação sensível seja trocada entre as mensagens.

10. POLÍTICAS INSTALAÇÃO DE SOFTWARES

10.1. Os usuários não poderão instalar ou fazer “upgrade” de qualquer espécie de programas ou aplicativos nas estações de trabalho sem aprovação do departamento de TI. É necessário seguir as seguintes obrigações:

10.1.1. Qualquer instalação, deverá ser solicitada diretamente ao departamento de TI, que deverá analisar com intuito de não causar conflito com banco de dados e outros softwares de uso corporativo.

10.1.2. Não será permitido carregar e executar qualquer tipo de jogo, áudio ou vídeo, bem como armazenar tais arquivos no servidor ou na estação de trabalho que não seja compatível com as atividades desenvolvidas.

10.1.3. Não será permitido o uso, para fins particulares ou de recreação, de serviços que sobrecarregam a rede da **EMBRAER PREV** tais como: rádios online, páginas de animação, visualização de apresentações, vídeos, jogos, conteúdo pornográfico, entre outros.

EMBRAER PREV – Sociedade de Previdência Complementar
Rua Euclides Miragaia, 145, Sala 1404 – Centro – CEP 12.245-820 – São José dos Campos - SP
Telefone: (12) 3307 7091

10.1.4. O departamento de TI está autorizado a retirar imediatamente, após comunicação por e-mail ao coordenador da equipe, qualquer software não autorizado que for encontrado em qualquer equipamento, independente de comunicação ao usuário ou a quem o instalou, e não responderá pelos danos que isso possa causar ao autor da instalação indevida.

11. POLÍTICAS DE UTILIZAÇÃO DO AMBIENTE DE REDE

11.1. A **EMBRAER PREV** disponibilizará os pontos de rede necessários ao desenvolvimento das atividades devendo, para qualquer alteração ou criação de um novo ponto haver solicitação em tempo hábil, seguindo as normas abaixo:

11.1.1. É vedado o uso de meios ilícitos de acesso aos computadores, sistemas e arquivos do ambiente de rede da **EMBRAER PREV**.

11.1.2. O acesso remoto aos computadores somente poderá ocorrer com o conhecimento ou consentimento do usuário, salvo se autorizado pelo departamento de TI da **EMBRAER PREV**.

11.1.3. Os arquivos, textos, planilhas ou imagens disponíveis na rede corporativa da **EMBRAER PREV** só poderão ser utilizados mediante o respeito aos direitos autorais, marcas registradas, patentes, sigilos comerciais ou outros direitos de propriedade intelectual de terceiros.

11.1.4. É vedada a utilização de recursos computacionais da **EMBRAER PREV** com o objetivo de obter proveito pessoal ou violar os sistemas de segurança estabelecidos.

12. POLÍTICA DE ACESSO A INTERNET

12.1. O usuário deve estar ciente das condutas vedadas que visam não comprometer o funcionamento da rede ou das estações de trabalho. São proibidas as seguintes atitudes:

12.1.1. Visualizar, criar, postar, carregar ou encaminhar quaisquer arquivos, ou mensagens de conteúdos abusivos, obscenos, insultuosos, material sexualmente tendencioso, pornográfico, difamatórios, agressivos, ameaçadores, vulgares, racistas, de apologia ao uso de drogas, de incentivo à violência ou outro material que possa violar qualquer lei aplicável.

12.1.2. Acessar salas de bate-papo, exceto se o acesso for necessário para realização das atividades do setor, mediante conhecimento do departamento de TI e autorização do coordenador responsável pela equipe.

12.1.3. Utilizar-se de quaisquer ferramentas para escutar músicas, vídeos ou jogos.

EMBRAER PREV – Sociedade de Previdência Complementar
Rua Euclides Miragaia, 145, Sala 1404 – Centro – CEP 12.245-820 – São José dos Campos - SP
Telefone: (12) 3307 7091

12.1.4. Fazer download de arquivos cujo conteúdo não tenha relação com as atividades desempenhadas pela **EMBRAER PREV**.

12.1.5. Utilizar-se de ferramentas que burlem a segurança e as regras de proxy/firewall, com o intuito de usufruir de serviços que não lhes são concedidos.

12.1.6. As responsabilidades e os procedimentos para gerenciar os ativos de rede são inteiramente do departamento de TI, que irá conceder somente os acessos necessários à atividade e minimizar danos causados por falha na operacionalização ou manutenção.

12.2. A instalação de AP- Access Points nas dependências da **EMBRAER PREV,** somente podem ser feitas pelo departamento de TI.

12.3. As conexões à rede da **EMBRAER PREV** devem ocorrer exclusivamente por meio de acesso autenticado.

12.4. O acesso à rede de visitantes da **EMBRAER PREV,** quando aplicável, será liberado somente para pessoas que não fazem parte do quadro de colaboradores, por meio de uma rede sem acesso interno.

13. POLÍTICA DE TRANSFERÊNCIA DE INFORMAÇÕES

13.1. Os requisitos para confidencialidade da informação estão descritos no Termo de confidencialidade e devem ser analisados criticamente quando houver mudança que afete estes requisitos.

13.2. Os colaboradores devem ser extremamente cautelosos na utilização de quaisquer meios de comunicação, ficando proibida qualquer troca de informações com o meio exterior sobre informações com mais alto grau de sensibilidade, sem autorização, justificativa ou criptografia.

14. POLÍTICA DE UTILIZAÇÃO DO E-MAIL

14.1. O acesso ao sistema de e-mail será disponibilizado aos usuários com solicitação prévia do coordenador/gerente da equipe ao RH, que irá passar para o departamento de TI para criação da conta de usuário com login e senha. A utilização do e-mail deverá se dar apenas como ferramenta de apoio às atividades profissionais, seguindo as seguintes orientações, não sendo permitidos:

14.1.1. Enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou da **EMBRAER PREV** vulneráveis às ações civis ou criminais.

EMBRAER PREV – Sociedade de Previdência Complementar
Rua Euclides Miragaia, 145, Sala 1404 – Centro – CEP 12.245-820 – São José dos Campos - SP
Telefone: (12) 3307 7091

14.1.2. Falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários, com o objetivo de evitar as punições previstas;

14.1.3. Apagar mensagens pertinentes de correio eletrônico quando a **EMBRAER PREV** estiver sujeita a algum tipo de investigação.

14.1.4. Produzir, transmitir ou divulgar mensagem que:

- Vise vigiar secretamente ou assediar outro usuário;
- Vise acessar informações confidenciais sem explícita autorização do proprietário;
- Vise acessar indevidamente informações que possam causar prejuízos a qualquer pessoa;
- Inclua imagens criptografadas ou de qualquer forma mascaradas;
- Tenha conteúdo considerado impróprio, obsceno ou ilegal.

14.2. É vetado o acesso ao e-mail corporativo por meio de aplicativos de e-mail não homologados pela tecnologia da informação.

15. POLÍTICA DE DESENVOLVIMENTO DE SOFTWARE

15.1. O desenvolvimento de sistemas deve ser realizado através de um processo formal e utilizando uma metodologia.

15.2. O desenvolvimento de sistemas deve ser realizado em ambiente de desenvolvimento separado e seguro e considerando também a segurança para cenários de reuso de código.

15.3. Os requisitos mínimos de segurança da informação para um sistema devem ser estabelecidos pela **EMBRAER PREV**.

15.4. A **EMBRAER PREV** deve adotar versões seguras para versionamento dos sistemas.

15.5. Os desenvolvimentos dos sistemas devem ser orientados a evitar, encontrar e corrigir vulnerabilidades.

16. POLÍTICA PARA PROTEÇÃO DE DADOS PESSOAIS

16.1. A **EMBRAER PREV,** deve garantir que o propósito do tratamento dos dados pessoais não seja ilícito ou abusivo.

16.2. A **EMBRAER PREV**, deve assegurar que os processos e os sistemas sejam projetados para que o tratamento de dados pessoais esteja limitado ao que é necessário ao propósito.

EMBRAER PREV – Sociedade de Previdência Complementar
Rua Euclides Miragaia, 145, Sala 1404 – Centro – CEP 12.245-820 – São José dos Campos - SP
Telefone: (12) 3307 7091

16.3. Devem ser observadas as legislações e regulamentações vigentes, que versam sobre:

16.3.1. Os direitos fundamentais à privacidade e à intimidade (Constituição Federal);

16.3.2. O habeas data, ação que permite ao indivíduo o conhecimento e a retificação de dados pessoais constantes de registros públicos ou banco de dados de entidades governamentais ou de caráter público;

16.3.3. A lei que dispõe sobre a apresentação e uso de documentos de identificação pessoal (lei nº 5.553);

16.3.4. Legislação bancária e fiscal;

16.3.5. Lei 10.406/2002 – Código Civil Brasileiro;

16.3.6. LGPD - Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709, de 14 de agosto de 2018 - Alterada pela Lei nº 13853, de 2019).

17. POLÍTICA DE PROTEÇÃO DE DADOS E BACKUP

17.1. A **EMBRAER PREV,** utiliza o One Drive e Sharepoint da Microsoft, para o serviço em nuvem que garante medidas de segurança da informação para proteger os seus arquivos.

17.2. Os arquivos são armazenados em serviços de nuvem da Microsoft, com gerenciamento de versões e lixeira em dois estágios para recuperação de dados.

17.3. Os arquivos, caso sejam excluídos, ficam armazenados durante 30 dias.

17.4. Não será realizado backup de informação armazenada em computadores.

17.5. As necessidades especiais de backup devem ser solicitadas ao departamento de TI.

17.6. O gestor da equipe deve solicitar ao departamento de TI a restauração da cópia de segurança, em caso de perda ou danos na informação.

17.7. Toda a necessidade de backup de arquivos da **EMBRAER PREV,** deve ser atendida pelo departamento de TI.

17.8. Os backups de banco de dados dos sistemas da **EMBRAER PREV,** são feitos pelos provedores de serviços externos.

17.9. As mídias devem ser submetidas a testes de recuperação periodicamente.

EMBRAER PREV – Sociedade de Previdência Complementar
Rua Euclides Miragaia, 145, Sala 1404 – Centro – CEP 12.245-820 – São José dos Campos - SP
Telefone: (12) 3307 7091

17.10. A **EMBRAER PREV** adota soluções tecnológicas e medidas que a protegem contra o vazamento de dados, monitorando a movimentação de dados e registrando a atividade de usuários no ambiente de arquivos corporativos.

17.11. Em possíveis atividades de mascaramento de dados devem ser alinhadas com a área de Tecnologia da Informação, visando garantir o uso adequado de tecnologias e métodos de mascaramento reconhecidos no mercado, que atendem requisitos satisfatórios de segurança da informação.

18. POLÍTICA PARA RELACIONAMENTO COM PROVEDORES EXTERNOS

18.1. Os requisitos de segurança da informação devem ser acordados com o provedor externo e documentados no Termo de Confidencialidade externo a fim de mitigar os riscos associados com o acesso dos provedores externos aos ativos da **EMBRAER PREV**.

18.2. O Termo de Confidencialidade externo firmado com o provedor deve contemplar todas as diretrizes desta política que são aplicáveis ao prestador de serviço

18.3. Para os serviços terceirizados de Tecnologia da Informação, este Termo de Confidencialidade externo deve ser estendido por toda a cadeia de suprimentos do provedor externo.

18.4. A aderência a esta política por parte do provedor externo deve ser monitorada sistematicamente pela **EMBRAER PREV.**

18.5. O Procedimento de Gestão de Provedor Externo, viabiliza esta política.

19. POLÍTICA PARA PROTEÇÃO CONTRA CÓDIGOS MALICIOSOS

19.1. A **EMBRAER PREV** adota soluções de proteção contra *malware*, com medidas de detecção e de prevenção.

19.2. Todos os servidores e estações de trabalho da **EMBRAER PREV** devem ter *software* antivírus instalado, ativado e atualizado sistematicamente.

19.3. Todos os colaboradores são responsáveis pela prevenção de contaminação da rede e em caso de identificação ou suspeita de vírus, deve solicitar uma análise, por meio de um processo formal.

19.4. Os colaboradores também são responsáveis pela não interrupção da verificação periódica dos sistemas de proteção contra vírus em suas estações de trabalho.

EMBRAER PREV – Sociedade de Previdência Complementar
Rua Euclides Miragaia, 145, Sala 1404 – Centro – CEP 12.245-820 – São José dos Campos - SP
Telefone: (12) 3307 7091

19.5. Em quaisquer situações, qualquer *software* ou arquivo proveniente de redes ou usuários externos deverão ser verificados por sistemas de proteção contra vírus.

20. POLÍTICA PARA CONTROLES CRIPTOGRÁFICOS E GERENCIAMENTO DE CHAVES

20.1 A **EMBRAER PREV**, quando aplicável, deve utilizar somente algoritmos de criptografia padronizados e extensivamente revisados.

20.2 O gerenciamento das chaves criptográficas públicas e privadas da **EMBRAER PREV** deve ser feito por uma Autoridade Certificadora (CA) confiável.

20.3 A **EMBRAER PREV** deve implementar um processo seguro para gerenciar o ciclo de vida de chaves criptográficas ou utilizar serviços e soluções homologadas que garantam a administração segura das chaves.

20.4 Salvo quando das atividades de infraestrutura de rede e desenvolvimento, o uso de criptografia na **EMBRAER PREV** não é uma necessidade das operações cotidianas, portanto, todo colaborador que precisar utilizar de algoritmos criptográficos deve solicitar apoio da Tecnologia da Informação.

21. POLÍTICA PARA USO DE SERVIÇOS EM NUVEM

21.1 Para aquisição de provedor de serviço em nuvem, as diretrizes para relacionamento com provedores externos devem ser respeitadas.

21.2 Quando aplicável, deve ser realizada avaliação de risco de segurança e privacidade da informação para identificar e tratar os riscos associados ao uso do serviço em nuvem.

21.3 A **EMBRAER PREV** deve avaliar e compreender a responsabilidade compartilhada e o esforço colaborativo pela segurança da informação e privacidade junto ao provedor de serviços em nuvem.

21.4 A **EMBRAER PREV** deve avaliar e compreender as suas responsabilidades e as do provedor de serviços em nuvem quanto aos controles de segurança da informação e de privacidade estabelecidos pela **EMBRAER PREV**.

EMBRAER PREV – Sociedade de Previdência Complementar
Rua Euclides Miragaia, 145, Sala 1404 – Centro – CEP 12.245-820 – São José dos Campos - SP
Telefone: (12) 3307 7091

21.5 A **EMBRAER PREV** deve se informar sobre como obter garantia da eficácia dos controles de segurança e privacidade da informação implementados pelo provedor de serviços em nuvem.

21.6 A **EMBRAER PREV** deve se informar sobre como alterar ou parar o uso dos serviços em nuvem.

21.7 A **EMBRAER PREV** deve avaliar o método utilizado pelo provedor de serviços em nuvem para fornecer, retornar e excluir as informações da **EMBRAER PREV**.

21.8 O contrato ou acordo entre a **EMBRAER PREV** e o provedor de serviços em nuvem deve abordar requisitos de confidencialidade, integridade e disponibilidade.

22. POLÍTICA PARA GESTÃO DE VULNERABILIDADES TÉCNICAS

22.1 As vulnerabilidades técnicas do ambiente da **EMBRAER PREV** devem ser identificadas por meio de um scanner de vulnerabilidades específico para este fim.

22.2 As ações requeridas para o tratamento das vulnerabilidades técnicas devem ser testadas e implementadas em tempo hábil e a eficácia destas ações deve ser verificada.

- O Procedimento Gestão de Vulnerabilidade Técnica integra o processo que viabiliza esta política.

23. POLÍTICA DE DIREITOS DE PROPRIEDADE INTELECTUAL

23.1 A **EMBRAER PREV** deve garantir o direito de propriedade intelectual dos produtos desenvolvidos internamente.

23.2 Nos contratos, deve ser estabelecida cláusula relacionada à propriedade intelectual da **EMBRAER PREV**.

24. POLÍTICA PARA USO DE INTELIGÊNCIA ARTIFICIAL

24.1 A **EMBRAER PREV**, se compromete a usar a IA de maneira ética e responsável, respeitando a transparência, justiça e a privacidade.

24.2 Todas as atividades relacionadas a IA devem cumprir as leis, regulamentos e normas aplicáveis, incluindo regulamentos de proteção de dados e propriedade intelectual.

EMBRAER PREV – Sociedade de Previdência Complementar
Rua Euclides Miragaia, 145, Sala 1404 – Centro – CEP 12.245-820 – São José dos Campos - SP
Telefone: (12) 3307 7091

24.3 A **EMBRAER PREV** é responsável por proteger a privacidade e segurança dos dados usados pelos sistemas de IA, de modo a garantir que dados confidenciais ou sensíveis não sejam utilizados sem o consentimento apropriado.

24.4 Deve ser mantida a transparência em relação ao uso de IA e a **EMBRAER PREV** deve ser responsável por todas as decisões baseadas nos resultados gerados por esses sistemas.

24.5 A IA não deve ser usada para criar conteúdo discriminatório ou prejudicial em relação à raça, gênero, religião, orientação sexual, entre outros.

25. PROCESSO DISCIPLINAR

O descumprimento de qualquer um dos tópicos deste documento sujeita o indivíduo às penalidades previstas no Código de Conduta Ética da **EMBRAER PREV**.

EMBRAER PREV – Sociedade de Previdência Complementar
Rua Euclides Miragaia, 145, Sala 1404 – Centro – CEP 12.245-820 – São José dos Campos - SP
Telefone: (12) 3307 7091