CONSELHO DE ADMINISTRAÇÃO DA EMPRESA DE TECNOLOGIA E INFORMAÇÕES DA PREVIDÊNCIA – DATAPREV S.A.

RESOLUÇÃO DE CONSELHO/CADM/008/2022

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE DATAPREV – PSIP

O Conselho de Administração da Empresa de Tecnologia e Informações da Previdência – DATAPREV S.A., no uso das atribuições que lhe foram conferidas no Estatuto Social da Empresa, aprovado pela 3ª Assembleia Geral Extraordinária da DATAPREV, em 13/11/2017, com alterações aprovadas na 2ª Assembleia Geral Ordinária da DATAPREV, realizada em 26 de abril de 2018, na 4ª Assembleia Geral Extraordinária, realizada em 19 de junho de 2018, na 7ª Assembleia Geral Extraordinária, realizada em 10 de abril de 2019, na 9ª Assembleia Geral Extraordinária, realizada em 10 de outubro de 2019, na 12ª Assembleia Geral Extraordinária, realizada em 29 de abril de 2020, na 14ª Assembleia Geral Extraordinária, realizada em 27 de outubro de 2020 e na 16ª Assembleia Geral Extraordinária, realizada em 11 de fevereiro de 2021, e,

CONSIDERANDO:

- A necessidade de atualização das diretrizes relativas à Segurança da Informação da DATAPREV.

RESOLVE:

Aprovar a Política de Segurança da Informação e Privacidade da DATAPREV – PSIP, conforme Anexo I desta Resolução.

Esta Resolução entra em vigor a partir desta data e revoga a Resolução de Conselho nº 011/2019.

Brasília, 01 de agosto de 2022.

CINARA WAGNER FREDO:00374753989

Assinado de forma digital por CINARA WAGNER FREDO:00374753989
Dados: 2022.09.05 14:01:50 -03'00'

CINARA WAGNER FREDO
Presidente

Documento assinado digitalmente
GUILHERME GASTALDELLO PINHEIRO SERR
Data: 23/09/2022 14:31:22-0300
Verifique em https://verificador.iti.br

GUILHERME GASTALDELLO PINHEIRO
Conselheiro

CHRISTIANE ALMEIDA EDINGTON:38769735549
Assinado de forma digital por CHRISTIANE ALMEIDA EDINGTON:38769735549
Dados: 2022.09.16 10:17:46 -03'00'

CHRISTIANE ALMEIDA EDINGTON
Conselheiro

ASSINADO DIGITALMENTE
FERNANDO ANDRE COELHO MITKIEWICZ
A conformidade com a assinatura pode ser verificada em:
http://serpro.gov.br/assinador-digital
SERPRO

FERNANDO ANDRÉ COELHO MITKIEWICZ
Conselheiro

ANTONIO CARLOS VILLELA SEQUEIRA:66749859704
Assinado de forma digital por ANTONIO CARLOS VILLELA SEQUEIRA:66749859704
Dados: 2022.09.05 15:08:14 -03'00'

ANTÔNIO CARLOS VILLELA SEQUEIRA
Conselheiro

NATALISIO DE ALMEIDA JUNIOR:94700257849
Digitally signed by NATALISIO DE ALMEIDA JUNIOR:94700257849
Date: 2022.09.06 14:28:45 -03'00'

NATALISIO DE ALMEIDA JUNIOR
Conselheiro

VENICIO DANTAS CAVALCANTI:66667712491
Assinado de forma digital por VENICIO DANTAS CAVALCANTI:66667712491
Dados: 2022.09.08 11:34:34 -03'00'

VENÍCIO DANTAS CAVALCANTI
Conselheiro

Anexo I

Política de Segurança da Informação e Privacidade da DATAPREV – PSIP [JF1]

1. Justificativa

Para cumprimento de sua missão social, a DATAPREV precisa assegurar que os dados sob sua guarda estejam adequadamente protegidos, a fim de que a execução e o aprimoramento das políticas sociais do Estado brasileiro, sejam perseguidas dentro do uso ético garantido, que exige controles e padrões de conduta para a obtenção de sucesso.

Com a privacidade já reconhecida como um direito de todo o cidadão, e sendo a segurança da informação requisito essencial para sua garantia, é imprescindível que uma política de segurança da informação e privacidade clara e abrangente, apoiada pela alta administração, esteja em curso para balizar todas as atividades da DATAPREV.

2. Objetivos

A Política de Segurança da Informação e Privacidade da DATAPREV tem como objetivos:

I. Estabelecer diretrizes estratégicas que orientem e apoiem as ações institucionais em segurança da informação e privacidade, com o intuito de preservar, em qualquer meio, a confidencialidade, integridade, disponibilidade e autenticidade dos dados, informações e conhecimentos produzidos ou custodiados pela empresa, em todo seu ciclo de vida;

II. Promover práticas de segurança da informação e privacidade, compatíveis com o uso aceitável das informações e dos ativos que as suportam, de forma a minimizar riscos e criar um ambiente seguro para a realização das atividades da empresa;

III. Promover o alinhamento das diretrizes de segurança da informação e privacidade com os objetivos e estratégias do negócio; e

IV. Garantir que os riscos cibernéticos e de privacidade sejam adequadamente endereçados.

3. Abrangência

A Política de Segurança da Informação e Privacidade da DATAPREV aplica-se a:

a) Todos os ambientes físicos pertencentes ao patrimônio ou sob a custódia da DATAPREV;

b) Todos os ambientes computacionais e ativos de informação pertencentes ou custodiados pela DATAPREV;

c) Todos os contratos, convênios, acordos, termos e outros instrumentos congêneres celebrados pela DATAPREV;

d) Todos os empregados, extraquadro, estagiários, jovens aprendizes e colaboradores de qualquer natureza jurídica e a quem, de alguma forma, execute atividades vinculadas à DATAPREV.

Esta Política também se aplica, no que couber, ao relacionamento da DATAPREV com outros órgãos e entidades públicos ou privados.

4. Referências

Constituem referências desta Política:

- Lei de Acesso à Informação – Lei nº 12.527, de 18 de novembro de 2011, Decreto nº 7.724, de 16 de maio de 2012 e Decreto nº 7.845, de 14 de novembro de 2012;
- Marco Civil da Internet – Lei nº 12.965, de 23 de abril de 2014 e Decreto nº 8.771, de 11 de maio de 2016;
- Lei Geral de Proteção de Dados Pessoais (LGPD) – Lei nº 13.709, de 14 de agosto de 2019;
- Estratégia Nacional de Segurança Cibernética – e-Ciber – Decreto nº 10.222, de 05 de fevereiro de 2020
- Política Nacional de Segurança da Informação – PNSI Decreto nº 9.832, de 12 de junho de 2019;
- Governança no compartilhamento de dados no âmbito da administração pública federal – Decreto nº 10.046, de 9 de outubro de 2019;
- Instrução Normativa GSI Nº 1, atualizada em 27 de maio de 2020;
- Instrução Normativa GSI/PR nº 3, de 28 de maio de 2021
- Normas Complementares da IN Nº1 do GSI, DSIC/GSI/PR nº 4 a n° 21;
- Portaria GSI/PR nº 93, de 18 de outubro de 2021 – Glossário de Segurança da Informação;
- Código de Conduta Ética e Integridade vigente;
- Política de Continuidade de Negócios da DATAPREV vigente;
- Política de Gestão de Riscos e Controles Internos vigente;
- Política de Integridade Corporativa da DATAPREV vigente;
- Política de Divulgação de informações da DATAPREV vigente;
- Política Anticorrupção vigente;
- Política de Porta-Vozes vigente;

- Norma Técnica ABNT NBR ISO/IEC 27000 – Tecnologia da Informação – Técnicas de Segurança;
- Norma Técnica ABNT/NBR ISO/IEC 27.001:2018 – Tecnologia da Informação – Técnicas de Segurança – Sistemas de Gerenciamento de Segurança da Informação – Visão Geral e Vocabulário – 5ª edição
- Norma Técnica ABNT/NBR ISO/IEC 27.002:2013 – Tecnologia da Informação – Técnicas de Segurança – Código de prática para controles de segurança da informação
- Norma Técnica ABNT/NBR ISO/IEC 27.701:2020 – Tecnologia da Informação – Técnicas de Segurança – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines
- Norma Técnica ABNT/NBR ISO/IEC 27.014:2013 – Tecnologia da Informação – Técnicas de Segurança – Governança de Segurança da Informação;
- Norma Técnica ABNT NBR 16167:2013 – Segurança da Informação – Diretrizes para classificação, rotulação e tratamento da informação;
- Norma Técnica ABNT NBR ISO/IEC 22301:2020 – Segurança da sociedade — Sistema de gestão de continuidade de negócios — Requisitos.

5 Princípios

São princípios básicos desta Política:

- A preservação da imagem da empresa e de seus empregados;
- A proteção dos dados pessoais para a garantia do direito individual e coletivo das pessoas à privacidade;
- A disseminação da cultura de segurança da informação e de privacidade;
- A promoção de um ambiente positivo de segurança, que seja construído sobre o comportamento humano
- Que o nível, a complexidade e os custos das ações de segurança da informação e privacidade sejam adequados ao valor dos ativos e informações, considerando os riscos a que estão expostos;
- Que as ações de Segurança da Informação e Privacidade da DATAPREV sejam integradas com os objetivos do negócio, com as demais ações dos órgãos da administração pública e sociedade civil e estejam alinhadas às diretrizes nacionais de segurança da informação; e
- Que a segurança da informação e privacidade estejam efetivamente incorporadas, desde a concepção e por todo o ciclo de vida, em todos os processos executados na DATAPREV.

6. Diretrizes

6.1 Responsabilidade e Comprometimento

Todos os empregados, extraquadro, estagiários, jovens aprendizes, colaboradores e aqueles que, de alguma forma, executem atividades vinculadas à DATAPREV são corresponsáveis pela proteção e salvaguarda das informações a que tenham acesso em razão da execução de suas atividades, independente das medidas de segurança.

Cabe a todos garantir o tratamento dos dados pessoais a que tenham acesso.

É responsabilidade de todos conhecer e cumprir as diretrizes definidas por esta Política e seus normativos.

6.2 Governança de Segurança da Informação e Privacidade

A Governança de Segurança deve direcionar as iniciativas de Segurança da Informação e Privacidade por toda a organização.

A Governança de Segurança da Informação deve garantir que o corpo diretivo receba informação relevante, dentro do contexto de negócios, sobre a segurança da informação, para permitir decisões pertinentes e oportunas sobre as questões de segurança, em apoio aos objetivos estratégicos da empresa.

6.3 Gestão de Riscos de Segurança da Informação e Privacidade

A gestão de riscos de segurança da informação e de privacidade deve ser realizada por meio de um processo contínuo, abrangendo as fases de análise, avaliação e tratamento dos riscos e a definição do escopo desta gestão deverá estar alinhada à Política de Gestão de Riscos Corporativos vigente.

6.4 Aspectos de Segurança na Gestão da Continuidade do Negócio

As ações de segurança da informação e de privacidade da DATAPREV devem estar alinhadas à Política de Continuidade de Negócios.

A DATAPREV deve estabelecer uma estrutura de gerenciamento adequada, planos, procedimentos de recuperação e resposta a desastres cibernéticos que visem a identificação de potenciais ameaças e a manutenção da segurança da informação e privacidade a níveis pré-determinados.

6.5 Classificação de Segurança e Tratamento da Informação

As informações produzidas e custodiadas devem ser classificadas de maneira a permitir o tratamento diferenciado, considerando o grau de importância, a criticidade, a sensibilidade e os requisitos legais, utilizando critérios definidos e observando o interesse público na informação.

O tratamento da informação, abrangendo todo o seu ciclo de vida, deve ser definido levando em conta as propriedades da disponibilidade, integridade, confidencialidade e autenticidade.

6.6 Controle de Acessos

Os acessos aos ambientes físicos e computacionais são controlados e registrados, devendo ser concedidos apenas a pessoas autorizadas, para o desempenho das atividades profissionais, sempre pautados nos princípios da necessidade de conhecer, privilégio mínimo e de privacidade, podendo ser revogados sem a obrigatoriedade de aviso prévio.

6.7 Uso Aceitável dos Ativos

A utilização de equipamentos e recursos computacionais, incluindo os pessoais, conectados à rede da DATAPREV ou nas dependências da empresa, é controlada e está sujeita a monitoração e eventual inspeção local.

As mensagens produzidas e transmitidas utilizando os recursos corporativos de comunicação eletrônica são propriedade da empresa.

Os serviços corporativos de correio eletrônico, comunicação unificada, Intranet e Internet devem ter seu uso orientado para as atividades de interesse da DATAPREV.

6.8 Educação e Conscientização

Esta Política e seus normativos devem ser divulgados para disseminar a cultura corporativa de Segurança da Informação e Privacidade.

Todos os alcançados por esta Política devem ser educados quanto ao uso adequado e seguro dos ativos e das informações a que tenham acesso.

Os profissionais que atuam nos processos de segurança da informação devem ser capacitados, alinhada às certificações profissionais e aos temas recomendados pelo DSI/GSI/PR.

A DATAPREV deve promover a conscientização em segurança da informação de todo o corpo funcional.

6.9 Contratações e Aquisições

Os contratos, acordos, convênios, ajustes e instrumentos congêneres, sempre que aplicável, deverão dispor de especificações de segurança da informação que definam, no mínimo, os direitos de propriedade das informações, a classificação de sigilo, estabeleçam as regras para transferência de informações e os termos de confidencialidade e não divulgação. Devem, ainda, prever a concordância com os procedimentos de segurança pelos seus empregados, prepostos ou representantes, sem prejuízo da participação em orientações complementares de segurança da informação que a DATAPREV julgar necessárias.

As contratações de tecnologia devem ser precedidas de análise de riscos e da classificação de segurança das informações, nos termos da legislação pertinente em vigor.

As contratações que envolvam a utilização de computação em nuvem devem conter cláusulas que estabeleçam a territorialidade de dados, garantam interoperabilidade, transferência e migração dos dados após seu encerramento.

6.10 Governança Segura de Dados

Devem ser implementados processos e controles adequados para assegurar que os dados sob responsabilidade da DATAPREV sejam tratados apenas para as finalidades para as quais foram coletados.

O acesso a dados custodiados deve ser regido pelos instrumentos contratuais firmados entre a DATAPREV e seus clientes, sem prejuízo do disposto na legislação vigente.

O compartilhamento de dados com outros órgãos da Administração Pública Federal restringe-se, estritamente, para execução de políticas públicas, cumprimento de demandas judiciais ou por força de lei cabendo a DATAPREV a definição dos níveis de segurança adequados.

É vedado o tratamento de informações classificadas em grau de sigilo ou custodiadas em ambiente de nuvem.

O tratamento em ambiente de nuvem de informações classificadas como vinculadas deve ser precedido de análise de riscos e, as medidas de mitigação devem ser implementadas antes da transferência dos dados.

O tratamento de dados pessoais em ambiente de nuvem deve ser precedido de análises de risco de segurança da informação e de análise de impacto à privacidade.

6.11 Privacidade e Proteção de Dados Pessoais

O tratamento de dados pessoais pela DATAPREV deve seguir os princípios de finalidade, adequação, necessidade, livre acesso, qualidade dos dados; transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas.

A DATAPREV deve implementar medidas para garantir os direitos dos titulares dos dados por ela custodiados, incorporando em seus processos de tratamento de dados pessoais controles para preservação da privacidade dos titulares.

6.12 Desenvolvimento Seguro

Os sistemas de informação desenvolvidos, internalizados e mantidos pela DATAPREV devem ter sua segurança especificada, analisada e testada, em todo seu ciclo de vida, e estar em conformidade com os requisitos contratuais e a legislação em vigor.

Na ausência de definições contratuais específicas, os direitos de propriedade de sistemas de informação bem como todo código-fonte desenvolvido são de propriedade da DATAPREV.

6.13 Tratamento e Resposta a Incidentes

Empregados, extraquadro, estagiários, jovens aprendizes e colaboradores da DATAPREV têm a obrigação de reportar, imediatamente, qualquer evento ou incidente de segurança que tenham conhecimento à Comissão responsável pelo tratamento e resposta a incidentes cibernéticos – CTIR.

Os eventos ou incidentes de segurança notificados ou detectados devem ser registrados e receber avaliação e tratamento.

Os incidentes que envolvam dados pessoais sob controle ou operados pela DATAPREV devem ser comunicados às partes interessadas, nos termos da legislação vigente.

6.14 Conformidade

Deve ser realizada a verificação de conformidade das práticas de segurança da informação da DATAPREV com esta Política e demais normativos e procedimentos agregados.

As atividades, produtos e serviços desenvolvidos pela DATAPREV devem estar em conformidade com leis, regulamentos, resoluções, normas, estatutos e contratos jurídicos vigentes, sejam eles internos, municipais, estaduais ou federais, inclusive os referentes à proteção das informações pessoais, profissionais e de terceiros.

O uso de sistemas, serviços e documentos deve estar em conformidade legal com direitos de propriedade intelectual e, portanto, com termos de licenciamento de instalação e uso pertinentes.

7. Penalidades

O não cumprimento das disposições constantes nesta Política de Segurança da Informação e Privacidade, suas normas e procedimentos agregados caracteriza infração, a ser apurada, sujeitando o infrator às penalidades previstas em lei e nos regulamentos internos da DATAPREV.

8. Atualização

A Política de Segurança da Informação e Privacidade deve ser revisada sempre que necessário ou em um intervalo não superior a 02 (dois) anos.

9. Disposições Finais

O detalhamento necessário à implementação desta Política está contido em normativos internos de segurança específicos.

Os casos omissos, as situações especiais e demais diretrizes necessárias à implantação desta Política devem ser analisados e deliberados pelo órgão responsável pela segurança da informação e privacidade na DATAPREV.

A DATAPREV deve manter esta Política e demais normativos internos de segurança e privacidade alinhados às diretrizes nacionais de segurança da informação e privacidade.

Esta Política dá ciência a todos que as ações executadas nos ambientes físicos, nos ambientes computacionais, nos ativos e nos recursos computacionais da DATAPREV poderão ser monitoradas e registradas, conforme previsto na legislação brasileira.

10. Glossário

Ativo	Meios de armazenamento, transmissão e processamento, sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso.
Ativo de Informação	Para efeito desta Política, denominado como “Ativo”.
Autenticidade	Propriedade de que a informação tenha sido produzida, expedida, recebida, modificada ou destruída por determinado indivíduo, equipamento ou sistema.
Colaboradores	Servidores e empregados públicos não requisitados, os fornecedores e prestadores de serviços.
Computação em Nuvem	Modelo computacional que permite acesso por demanda, e independentemente da localização, a um conjunto compartilhado de recursos configuráveis de computação (rede de computadores, servidores, armazenamento, aplicativos e serviços), provisionados com esforços mínimos de gestão ou interação com o provedor de serviços.
Comunicação Unificada	Solução de comunicação que integra dados, voz e vídeo, até mesmo de forma remota, por meio de dispositivos fixos e móveis, unificando os locais da empresa numa única plataforma de comunicação.

Confidencialidade	Propriedade de que a informação não seja revelada à pessoa física, sistema, órgão ou entidade não autorizado e credenciado.
Dado Pessoal	Informação relacionada a pessoa natural identificada ou identificável.
Dado Pessoal Sensível	Dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.
Disponibilidade	Propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade.
Empregado	Entende-se como empregado, para fins desta Política, o empregado contratado, o titular de cargo de direção e assessoramento, o ocupante de cargo em comissão ou função de confiança, o empregado ou servidor cedido ou requisitado.
Evento de Segurança	Ocorrência identificada de um sistema, serviço ou rede, que indica uma violação da Política de Segurança da Informação ou falha de controles, ou uma situação desconhecida, que possa ser relevante para a segurança da informação.
Extraquadro	Empregados contratados com características de demissibilidade ad nutum e os requisitados da administração pública.
Governança de Segurança da Informação	Sistema pelo qual as atividades de segurança da informação são dirigidas e controladas
Incidente	Qualquer evento que não faça parte da operação padrão de um serviço e que causa, ou pode causar, uma interrupção do serviço ou uma redução da sua qualidade.
Incidente de Segurança	Qualquer evento de segurança adverso, confirmado ou sob suspeita, que indique violação da Política de Segurança da Informação e Privacidade da DATAPREV, levando à perda de um ou mais dos princípios básicos de Segurança da Informação: Confidencialidade, Integridade e Autenticidade.
Informação	Dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato.

Informação Classificada	Informação sigilosa em poder dos órgãos e entidades públicas, observado o seu teor e em razão de sua imprescindibilidade à segurança da sociedade ou do Estado, classificada como ultrassecreta, secreta ou reservada, conforme procedimentos específicos de classificação estabelecidos na legislação vigente. Para os fins desta Política é toda informação classificada em grau de sigilo nos termos da LAI.
Informação Custodiada	Informações sob guarda da DATAPREV provenientes de atividades finalísticas dos clientes.
Informação Pessoal	Informação relacionada à pessoa natural identificada ou identificável, relativa à intimidade, vida privada, honra e imagem.
Informação Vinculada	A informação que faça parte de um contexto regulamentado por alguma legislação específica.
Integridade	Propriedade de que a informação não foi modificada, inclusive quanto à origem e ao destino, ou destruída.
Necessidade de Conhecer	Condição segundo a qual o conhecimento da informação é indispensável para o adequado exercício de cargo, função, emprego ou atividade.
Privacidade	Propriedade do que é privado, do que diz respeito a alguém em particular
Privilégio Mínimo	Concessão de recursos e autorizações mínimos em um sistema de informação necessários para o adequado exercício de cargo, função, emprego ou atividade.
Risco de Segurança	Potencial associado à exploração de uma ou mais vulnerabilidades de um ativo de informação ou de um conjunto de tais ativos, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização.
Tratamento de Riscos	Processo de seleção e implementação de ações de segurança da informação e comunicações para evitar, reduzir, reter ou transferir um risco.