FUNDAÇÃO DE PREVIDÊNCIA COMPLEMENTAR DO SERVIDOR PÚBLICO FEDERAL DO PODER EXECUTIVO

Funpresp

POLÍTICA DE GESTÃO

E SEGURANÇA DA INFORMAÇÃO

Brasília/DF

Aprovada pelo Conselho Deliberativo na 127ª Reunião Ordinária, de 22 de setembro de 2023, Resolução nº 596.

Vigência: 25/10/2023

SUMÁRIO

CAPÍTULO I – DISPOSIÇÕES PRELIMINARES 3
Seção I - OBJETIVOS 3
Seção II - APLICAÇÃO 3
Seção III - REFERÊNCIAS 4
Seção IV - DEFINIÇÕES 4
CAPÍTULO II – SISTEMA DE GESTÃO E SEGURANÇA DE INFORMAÇÃO 7
Seção I - PRINCÍPIOS 7
Seção II - RESPONSABILIDADES 8
Seção III - GARANTIA E CONTROLE DE ACESSO 9
Seção IV - SEGURANÇA FÍSICA E DO AMBIENTE 10
10Seção V - CONFORMIDADE 11
Seção VI - GESTÃO DE RISCOS E INCIDENTES DE SEGURANÇA DA INFORMAÇÃO 11
Seção VII - SEGURANÇA EM TECNOLOGIA DA INFORMAÇÃO 12
Seção VIII - CONSCIENTIZAÇÃO E CAPACITAÇÃO 12
CAPÍTULO III – GESTÃO DOCUMENTAL 13
CAPÍTULO IV – DISPOSIÇÕES FINAIS 13

O CONSELHO DELIBERATIVO DA FUNDAÇÃO DE PREVIDÊNCIA COMPLEMENTAR DO SERVIDOR PÚBLICO DO PODER EXECUTIVO FEDERAL, NO USO DAS ATRIBUIÇÕES QUE LHE CONFERE O INCISO I DO ART. 34 DO ESTATUTO, RESOLVE ESTABELECER OS PRINCÍPIOS E DIRETRIZES RELACIONADOS À GESTÃO E SEGURANÇA DA INFORMAÇÃO.

CAPÍTULO I

DISPOSIÇÕES PRELIMINARES

Seção I

OBJETIVOS

Art. 1°. A Política de Gestão e Segurança da Informação tem por objetivo estabelecer princípios, responsabilidades e competências relativas à gestão e à segurança da informação, visando assegurar a integridade, a confidencialidade, a disponibilidade e a autenticidade das informações, bem como minimizar os riscos de falhas, danos, acessos indevidos ou prejuízos que possam comprometer a continuidade do fluxo de informações.

Art. 2°. As diretrizes da Gestão da Informação visam preservar e proteger as informações da Funpresp-Exe, de forma a manter sua confidencialidade, garantir que não seja modificada ou perdida, além de assegurar sua disponibilidade no caso de necessidade e pertinência.

§ 1° Todos os ativos de informação coletados, produzidos, recebidos, utilizados, em tramitação e armazenados devem ser tratados com eficiência e eficácia, de modo seguro e transparente, alinhados às exigências legais e de fiscalização, bem como à privacidade e proteção de dados pessoais.

§ 2° A Gestão da Informação contemplará os critérios e procedimentos para a preservação física e digital do acervo institucional.

Art. 3°. As diretrizes da Segurança da Informação aplicáveis aos ambientes, pessoas e processos da Funpresp-Exe visam proteger os ativos de informação produzidos e custodiados pela Fundação nos aspectos relativos ao ambiente físico e de tecnologia da informação, independentemente de onde eles se encontrem.

Seção II

APLICAÇÃO

Art. 4°. As disposições desta Política aplicam-se aos profissionais da Funpresp-Exe, membros dos órgãos colegiados estatutários e regimentais, e, no que couber, aos prestadores de serviços e fornecedores no exercício de suas atividades, bem como ao ambiente de tecnologia da informação da Funpresp-Exe.

Parágrafo único. A segurança da informação abrange aspectos físicos, tecnológicos

e humanos.

Seção III

REFERÊNCIAS

Art. 5°. Devem ser utilizados como instrumentos de boas práticas técnicas e gerenciais, no que couber, as seguintes referências:

I – Lei Complementar n° 109/2021;

II – Lei n° 12.527/2011 – Lei de Acesso à Informação;

III – Lei nº 12.965/2014 – Marco Civil da Internet;

IV – Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais;

V – Lei n° 14.129/2021 – Lei do Governo Digital;

VI – Resolução PREVIC nº 23, de 14 de agosto de 2023;

VII – Código de Ética e de Conduta da Funpresp-Exe;

VIII – Política de Alçadas da Funpresp-Exe;

IX – Política de Gestão da Integridade, Riscos e Controles Internos;

X – Política de Privacidade e de Proteção de Dados;

XI – Manual de Orientação ao Empregado da Funpresp-Exe;

XII – Matriz de Competências da Funpresp-Exe;

XIII – Norma ABNT NBR ISO/IEC 27002:2013; e

XIV – Norma ABNT NBR ISO/IEC 27005:2019.

Seção IV

DEFINIÇÕES

Art. 6°. Para fins desta Política, entende-se por:

I – ASSINATURA DIGITAL: método de autenticação de informação digital tipicamente tratada como substituta à assinatura física;

II – ATIVOS DE INFORMAÇÃO: componente (humano, tecnológico, físico ou lógico) que sustenta um ou mais processos de negócio de uma unidade ou área de negócio da Funpresp-Exe;

III – AUTENTICIDADE: garantia da identidade de quem envia a informação e a veracidade da fonte da informação;

IV – CONFIDENCIALIDADE: capacidade de assegurar que informações não estejam disponíveis e não sejam reveladas às pessoas, sistemas,

órgãos ou entidades não autorizados ou credenciados;

V – CONTROLE DE ACESSO: processo computacional para autenticação da credencial de um usuário, autorizando o uso do recurso com base no seu perfil de acesso;

VI – DADO: matéria-prima da informação, que isoladamente transmite uma mensagem ou representa algum conhecimento;

VII – DADOS PESSOAIS: informação relacionada a pessoa natural identificada ou identificável, na forma da legislação vigente;

VIII – DISPONIBILIDADE: acessibilidade que se tem aos dados e sistemas, os quais podem ser consultados a qualquer momento pelos usuários autorizados;

IX – DOCUMENTO: unidade de registro de informações, qualquer que seja o suporte ou formato;

X – FALHA NA SEGURANÇA DA INFORMAÇÃO: causa potencial de um incidente ou fragilidade na gestão da segurança que pode resultar em dano para o fluxo de informação da Fundação;

XI – GESTÃO DA INFORMAÇÃO: ciclo de atividade organizacional, a aquisição de informações a partir de uma ou mais fontes, a custódia e o trâmite de informações e a sua melhor disposição por meio de arquivamento ou eliminação;

XII – GESTORES: gerentes e coordenadores da Funpresp-Exe;

XIII – INCIDENTE DE SEGURANÇA DA INFORMAÇÃO: indício ou ocorrência que comprometa, real ou potencialmente, a disponibilidade, a integridade, a confidencialidade ou a autenticidade de sistema de informação ou suas informações, ou tentativa de exploração de vulnerabilidade que viola norma, política, procedimento de segurança ou política de uso;

XIV – INCIDENTE DE SEGURANÇA COM DADOS PESSOAIS: qualquer evento adverso, confirmado ou sob suspeita, relacionado à violação de dados pessoais, sendo acesso não autorizado, acidental ou ilícito que resulte em destruição, perda, alteração, vazamento ou qualquer forma de tratamento de dados ilícita ou inadequada, que tem a capacidade de pôr em risco os direitos e as liberdades dos titulares dos dados pessoais;

XV – INFORMAÇÃO: todo o conjunto de dados devidamente ordenados e organizados de forma a terem significado;

XVI – INFORMAÇÕES CUSTODIADAS: informações sob a responsabilidade da Funpresp-Exe cedidas pelo seu proprietário em razão

de contrato, acordo, convênio ou ajuste;

XVII – INFORMAÇÃO PÚBLICA: refere-se à informação publicamente acessível, cuja utilização não infringe qualquer direito legal ou qualquer obrigação de confidencialidade;

XVIII – INFORMAÇÃO NÃO-PÚBLICA: aquela imprescindível à segurança das atividades da Fundação e que diga respeito à intimidade, vida privada, honra e imagem, bem como que se enquadre nas hipóteses de sigilo previstas em legislação específica;

XIX – INTEGRIDADE: preservação da precisão, confiabilidade e consistência das informações e sistemas ao longo do ciclo de atividade organizacional;

XX – PARTES ENVOLVIDAS: Participantes, assistidos, beneficiários, patrocinadores, profissionais, membros dos órgãos colegiados estatutários e regimentais, sociedade, prestadores de serviços, bem como entidades representativas de classes ligadas à Funpresp-Exe;

XXI – PROFISSIONAL: empregado contratado sob o regime da CLT, empregado ou servidor público cedido à Funpresp-Exe e estagiário;

XXII – RECURSOS COMPUTACIONAIS: conjunto de hardware e software em que dados e informações são processados, armazenados ou transmitidos;

XXIII – RISCOS DE SEGURANÇA: probabilidade da ocorrência de um incidente de segurança da informação ponderado com o respectivo impacto;

XXIV – SEGURANÇA DA INFORMAÇÃO: conjunto de procedimentos que visa garantir a integridade, a confidencialidade, a disponibilidade e a autenticidade das informações, bem como minimizar os riscos de falhas, danos, acessos indevidos ou prejuízos que possam comprometer a continuidade do fluxo de informações;

XXV – SEGURANÇA FÍSICA E PATRIMONIAL: conjunto de procedimentos que visa prevenir danos e interferências nas instalações da Funpresp-Exe que possam causar perda, roubo ou comprometimento das informações;

XXVI – SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO: serviços disponíveis na rede corporativa, acessíveis por meio de credencial da rede, tais como intranet, internet, correio eletrônico, servidor de arquivos e sistemas corporativos;

XXVII – SIGILO: propriedade de que a informação não seja revelada à pessoa física ou jurídica, sistema, órgão ou entidade não autorizado e

credenciado;

XXVIII – TERMO DE RESPONSABILIDADE DE ACESSO: instrumento a ser assinado por todos usuários, em que dão ciência sobre as diretrizes da Política de Gestão e Segurança da Informação e se responsabilizam pelo acesso e uso dos recursos computacionais da Funpresp-Exe;

XXIX – USUÁRIOS: toda pessoa física que utiliza bem ou serviço da Funpresp-Exe, assim como ferramentas ou dispositivos para se comunicar com outras pessoas, escrever, disponibilizar ou publicar documentos;

XXX – VIOLAÇÃO DA SEGURANÇA DA INFORMAÇÃO: qualquer incidente como fraude, sabotagem, espionagem, desvio, falha ou evento indesejado ou inesperado que resulte em acesso não autorizado a dados, aplicativos, redes, sistemas ou dispositivos, de modo a comprometer ou ameaçar a segurança da informação;

XXXI – VULNERABILIDADE: condição que, quando explorada por um atacante ou por acessos não autorizados, seja proveniente de situações acidentais ou ilícitas, pode resultar em uma violação de segurança.

CAPÍTULO II

SISTEMA DE GESTÃO E SEGURANÇA DE INFORMAÇÃO

Seção I

PRINCÍPIOS

Art. 7°. As ações relacionadas com a gestão e com a segurança de informação da Funpresp-Exe serão norteadas pelos seguintes princípios:

I – ADEQUAÇÃO: compatibilidade do tratamento dos dados com as finalidades informadas ao titular do dado, em concordância ao contexto do tratamento;

II – CELERIDADE: oferecimento de respostas rápidas a incidentes e falhas de gestão e segurança da informação;

III – CLAREZA: as regras, documentações e comunicações devem ser precisas, concisas e de fácil entendimento às partes envolvidas;

IV – CONTINUIDADE DAS ATIVIDADES: o serviço prestado pela Funpresp-Exe não pode sofrer interrupções repentinas e continuadas;

V – EFICÁCIA: relação entre os resultados alcançados e os planejados;

VI – EFICIÊNCIA: a adequação dos custos das ações de segurança da informação e comunicação ao valor das informações a serem protegidas;

VII – ÉTICA: refere-se às regras e preceitos de ordem valorativa e moral das pessoas, sendo pré-requisito e suporte para a geração de confiança;

VIII – LEGALIDADE: refere-se às atribuições estatutárias, regimentais, bem como às leis, políticas e normas organizacionais, administrativas, técnicas e operacionais da Funpresp-Exe;

IX – NECESSIDADE: limitação do acesso aos dados ao mínimo necessário para a realização de sua finalidade;

X – PESSOALIDADE: o acesso aos ativos da informação é pessoal e intransferível;

XI – PRIVACIDADE: garantia ao direito pessoal e coletivo, à intimidade e ao sigilo da correspondência e das comunicações individuais além da preservação da imagem da Funpresp-Exe e de suas partes envolvidas;

XII – PREVENÇÃO: adoção das medidas necessárias para mitigar a ocorrência de danos em virtude do tratamento de dados pessoais;

XIII – PUBLICIDADE: transparência no trato da informação, observados os critérios legais;

XIV – RESPONSABILIZAÇAO DO PROPRIETÁRIO DOS ATIVOS: consideração do usuário como proprietário dos ativos de informação sob sua responsabilidade, bem como responsável pela liberação e cancelamento do acesso, classificação de segurança e medidas de proteção de informação e dados;

XV – RESTRIÇÃO DE ACESSO E USO DE ATIVOS: garantia de que o acesso e uso dos ativos sejam controlados e limitados às atribuições necessárias para o cumprimento das finalidades profissionais;

XVI – SEGURANÇA: utilização de medidas técnicas e administrativas aptas a proteger os dados de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão; e

XVII – UTILIDADE DO ACESSO AOS ATIVOS DE INFORMAÇÃO: o acesso deve ser concedido de acordo com a utilidade para o usuário e preservado com sigilo.

Seção II

RESPONSABILIDADES

Art. 8°. A Funpresp-Exe deve utilizar sua estrutura organizacional para assegurar o cumprimento dos princípios desta política em prol da segurança da informação, definindo papéis e responsabilidades, conforme a seguir:

I – GERÊNCIA DE TECNOLOGIA E INFORMAÇÃO: responsável por gerenciar o servidor de dados, por promover a cultura da Segurança da Informação Tecnológica, por gerir as regras de proteção dos equipamentos de infraestrutura tecnológica, propondo a revisão nas respectivas normas;

II – UNIDADES ORGANIZACIONAIS: responsáveis por orientar o cumprimento desta Política no âmbito de suas atribuições, bem como manter a Gerência de Tecnologia e Informação informada acerca dos níveis de acessos referentes aos usuários sob sua supervisão; e

III – USUÁRIOS: responsáveis por notificar eventuais incidentes de segurança e pelo cumprimento desta Política e demais normativos relacionados à gestão e à segurança da informação, no âmbito de suas atribuições, por meio do uso de forma responsável, profissional, ética e legal dos ativos de informação, respeitando os direitos e as permissões de uso concedidas pela Funpresp-Exe.

Seção III

GARANTIA E CONTROLE DE ACESSO

Art. 9º. O acesso aos sistemas de informação da Funpresp-Exe deve ser controlado de acordo com o valor, sensibilidade e criticidade da informação, e deve considerar aspectos de restrições legais e normativas.

Art. 10. O processo de controle de acesso à informação tem por objetivo garantir que o acesso físico e lógico à informação seja franqueado exclusivamente a pessoas autorizadas, com base nos requisitos de negócio e de segurança da informação, assegurando a segregação de funções e a devida responsabilização pela liberação e cancelamento de acessos, classificação de segurança e medidas de proteção de informação e dados.

§ 1º O acesso às informações não-públicas produzidas ou custodiadas pela Funpresp-Exe deve permanecer restrito às pessoas que tenham necessidade de conhecê-las.

§ 2º O acesso às informações não-públicas por quaisquer usuários é condicionado ao aceite de termo de sigilo e responsabilidade.

Art. 11. Todos os usuários que manipulem ou tenham acesso a informações sob custódia ou de propriedade da Funpresp-Exe devem garantir a confidencialidade e o sigilo dessas informações, de acordo com os requisitos legais, de negócio e de segurança da informação disciplinados em normativos específicos.

Parágrafo único. Deve-se adotar comportamento ético e seguro, evitando assuntos sigilosos em ambientes sociais e particulares, impressão, transmissão, compartilhamento e transporte para fora das instalações da Funpresp-Exe de informação sem autorização.

Art. 12. As informações institucionais devem, necessariamente, ser gravadas nos servidores de rede da Funpresp-Exe.

Art. 13. A conexão de quaisquer dispositivos móveis particulares à rede interna da Funpresp-Exe somente é permitida para o exercício das atividades laborais, mediante acesso seguro e autenticado a serviços disponibilizados pela Gerência de Tecnologia e Informação, desde que não infrinja quaisquer outros regramentos desta Política ou demais normativos internos.

Art. 14. A Fundação deve estabelecer em seus contratos, acordos, convênios ou ajustes, cláusulas específicas sobre sigilo, em especial quando informações forem disponibilizadas a terceiros, que assegurem a observância desta Política e suas normas e protejam os dados e informações recebidas contra a utilização indevida, a intercepção, cópia, modificação não autorizada, indisponibilidade, desvio ou destruição, consignando que a infringência pode ensejar responsabilização cível, administrativa e penal.

Art. 15. Compete ao terceiro, parceiro ou fornecedor, adotar medidas preventivas e controles adequados para manutenção da confidencialidade, integridade e disponibilidade da informação em qualquer meio nos ambientes de execução do contrato durante sua vigência.

Seção IV

SEGURANÇA FÍSICA E DO AMBIENTE

Art. 16. A segurança física e do ambiente, disposta em normativo específico, tem por objetivo, em relação à segurança da informação, prevenir danos e interferências nas instalações da Funpresp-Exe que possam causar perda, roubo ou comprometimento das informações.

Art. 17. Para garantir a segurança física e do ambiente, serão estabelecidos, no mínimo, controles relacionados às seguintes ações:

I – prevenir o acesso físico indevido e sem autorização, bem como danos e interferências nas instalações e informações da Funpresp-Exe;

II – assegurar que membros dos órgãos colegiados estatutários e regimentais, profissionais e quaisquer outros usuários da Fundação entendam suas responsabilidades e assinem termos de segurança da informação, com a finalidade de reduzir os riscos de burla, falhas humanas, furto, roubo, fraude ou manipulação indevida dos ativos de informação da Funpresp-Exe; e

III – evitar o trânsito indevido de pessoas alheias ao quadro funcional no ambiente operacional de trabalho.

Art. 18. A segurança física e do ambiente contempla a proteção do patrimônio contra sinistros que possam causar danos às instalações e/ou equipamentos da Funpresp-

Exe, como incêndios, vazamentos de água, umidade, deterioração de documentos, entre outros.

Seção V

CONFORMIDADE

Art. 19. Devem ser adotados procedimentos apropriados para garantir a conformidade e o respeito às exigências legais quanto à disponibilização de informações, bem como ao uso e disseminação de informações protegidas por leis.

Art. 20. Os sistemas de informação da Funpresp-Exe, além de disponibilizar os registros em prazos e formatos que atendam às exigências legais, devem protegê-los contra perda, acesso indevido, destruição e falsificação, visando à salvaguarda dos ativos de informação.

Seção VI

GESTÃO DE RISCOS E INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Art. 21. A gestão de riscos e incidentes em segurança da informação tem por objetivo assegurar que fragilidades e incidentes em segurança da informação sejam identificados e notificados, para permitir a tomada de ação em tempo hábil.

Art. 22. Qualquer incidente relacionado à garantia ou ao controle de acesso aos sistemas tecnológicos, identificado por qualquer profissional, deve ser imediatamente comunicado ao seu superior imediato ou substituto e à Gerência de Tecnologia e Informação para avaliação e determinação das ações que se fizerem necessárias.

Parágrafo único. Os membros estatutários, regimentais e os gestores que tenham ciência ou suspeita de qualquer incidente devem informar imediatamente à Gerência de Tecnologia e Informação, além de colaborar, na respectiva área de competência, com a identificação e o tratamento de incidentes em segurança da informação.

Art. 23. Qualquer incidente ou vulnerabilidade que possa envolver dados pessoais, identificado por qualquer profissional, deve ser imediatamente comunicado à Gerência de Tecnologia e Informação para avaliação e determinação das ações que se fizerem necessárias.

Art. 24. Os incidentes e vulnerabilidades comunicados à Gerência de Tecnologia e Informação serão avaliados e, havendo a possibilidade de envolvimento de dados pessoais, serão comunicados ao Encarregado pela Proteção de Dados indicando a detecção do incidente e as medidas para correção, entre outras providências cabíveis.

Art. 25. Os serviços de tecnologias classificados como críticos devem ser monitorados e eventuais incidentes registrados no intuito de permitir uma análise posterior para identificar as causas e promover melhoria contínua aos serviços, sistemas e controles.

Art. 26. Para garantir a continuidade das operações essenciais e a recuperação do

fluxo de informações, planos e procedimentos devem ser estabelecidos para impedir a interrupção das atividades de negócios e para proteger os processos críticos contra incidentes, falhas e danos, devendo atender aos seguintes requisitos:

I - avaliação em regime emergencial das consequências de desastres, falhas de segurança e perda de serviços;

II - contingência e recuperação do funcionamento normal dentro de períodos de tempo determinados; e

III - recuperação tempestiva das operações consideradas essenciais.

Seção VII

SEGURANÇA EM TECNOLOGIA DA INFORMAÇÃO

Art. 27. Compete à Gerência de Tecnologia e Informação monitorar e revisar periodicamente os procedimentos acerca do uso de recursos de tecnologia da informação, controle de acesso, e-mail, uso da internet, uso de antivírus, acesso remoto e acesso a serviços de tecnologia da informação por terceiros.

Parágrafo único. Deverão ser adotadas medidas preventivas e de proteção contra acesso tecnológico indevido.

Art. 28. A assinatura digital de documentos deve ser realizada preferencialmente por meio da utilização de usuário (*login*) e senha fornecidos mediante procedimento de cadastro no qual esteja assegurada a adequada identificação do interessado, que deverá ser disciplinada em normativo específico, sem prejuízo de outras assinaturas eletrônicas juridicamente válidas.

Seção VIII

CONSCIENTIZAÇÃO E CAPACITAÇÃO

Art. 29. As diretrizes básicas da Política de Gestão e Segurança da Informação devem ser amplamente divulgadas, visando que todos os usuários tenham consciência de seu conteúdo e responsabilidade por sua condução.

Parágrafo único. A concessão de acesso aos sistemas de informação da Funpresp-Exe depende da assinatura do Termo de Responsabilidade de Acesso pelo usuário, que será firmada tão logo constituído vínculo com a Funpresp-Exe.

Art. 30. Os profissionais, membros dos órgãos estatutários e regimentais e demais usuários devem ser continuamente capacitados sobre o uso dos ativos de informação por ocasião da realização de suas atividades.

Art. 31. Os treinamentos a serem disponibilizados devem estar compatíveis com as tecnologias atualmente implementadas no ambiente informatizado e com as demais que porventura venham a ser adotadas.

CAPÍTULO III

GESTÃO DOCUMENTAL

Art. 32. De forma complementar à Política de Gestão e Segurança da Informação, será estabelecido normativo de gestão documental, para definir os procedimentos de criação, classificação, grau de sigilo, tramitação, acesso à informação, digitalização, arquivamento, destruição, tabela de temporalidade, os procedimentos inerentes à formação de dossiês, processos administrativos e a gestão do acervo documental físico e eletrônicos da Funpresp-Exe.

Art. 33. Compete a todos os profissionais e quaisquer outros usuários que tenham acesso às informações da Funpresp-Exe executar os procedimentos relativos à gestão dos acervos sob suas responsabilidades, conforme disciplinado no normativo de gestão documental, observando sobretudo a classificação dos documentos, a fim de cumprir, no que couber, os critérios definidos nas Leis nºs 12.527/2011 - Lei de Acesso a Informação e 13.709/2018 – Lei Geral de Proteção de Dados Pessoais.

Parágrafo Único. O uso e manutenção de dados, documentos e informações digitais de conteúdo institucional devem ser armazenados nos servidores de rede, observando os padrões de arquivamento digital estabelecidos nos normativos da Funpresp-Exe.

CAPÍTULO IV

DISPOSIÇÕES FINAIS

Art. 34. O descumprimento das disposições constantes nesta Política e nas normas complementares sobre gestão e segurança da informação caracteriza infração funcional, a ser apurada nos termos dos normativos internos vigentes, sem prejuízo da responsabilidade penal.

Art. 35. Os regramentos estabelecidos nesta Política de Gestão e Segurança da Informação adotados pela Funpresp-Exe deverão ser publicados para amplo conhecimento de seus usuários.

Art. 36. As informações produzidas e as soluções tecnológicas desenvolvidas por quaisquer usuários da Funpresp-Exe, no exercício de suas atribuições, são patrimônio intelectual da Fundação e não cabe a seus criadores qualquer forma de direito autoral, ressalvado o reconhecimento da autoria, se for o caso.

Art. 37. Esta Política entra em vigor na data de sua publicação.

Controle de versões

Revisão	Data
2.0	25/10/2023