RS PREV
FUNDAÇÃO DE PREVIDÊNCIA COMPLEMENTAR DO SERVIDOR PÚBLICO DO ESTADO DO RIO GRANDE DO SUL

DIRETORIA-EXECUTIVA

Resolução nº 03, de 11 de agosto de 2022

Estabelece a Política de Gestão e Segurança da Informação da Fundação de Previdência Complementar do Servidor Público do Estado do Rio Grande do Sul - RS-Prev.

A Diretora-Presidente da Fundação de Previdência Complementar do Servidor Público do Estado do Rio Grande do Sul – RS-Prev, no uso de suas atribuições legais, previstas no Estatuto, artigo 57, incisos VI e IX, registra que a Diretoria-Executiva, em sua 231ª Reunião Ordinária, realizada em 11 de agosto de 2022, RESOLVEU:

Art. 1º Fica estabelecida a Política de Gestão e Segurança da Informação no âmbito da Fundação de Previdência Complementar do Servidor Público do Estado do Rio Grande do Sul – RS-Prev, conforme ANEXO ÚNICO.

Art. 2º Esta Resolução entra em vigor na data de sua aprovação.

Assinado de forma digital por DANIELLE CRISTINE DA SILVA:••••••••••

Danielle Cristine da Silva
Diretora-Presidente

ANEXO ÚNICO

POLÍTICA DE GESTÃO E SEGURANÇA DA INFORMAÇÃO

1. APRESENTAÇÃO

1.1. A Política de Gestão e Segurança da Informação – PGSI servirá de guia para a implantação de medidas de proteção que deverão ser aplicadas a toda e qualquer informação da Fundação de Previdência Complementar do Servidor Público do Estado do Rio Grande do Sul – RS-Prev, independentemente de onde ela se encontre armazenada, para fins de resguardo da imagem e de modo a assegurar o pleno cumprimento dos objetivos institucionais da Fundação.

1.2. Estas orientações devem ser lidas, entendidas e seguidas por todos os níveis hierárquicos da RS-Prev, para que as informações tenham o grau de autenticidade, disponibilidade, confidencialidade e integridade exigidos nesta Política.

2. DEFINIÇÕES

2.1. Para fins desta Política, entende-se por:

I – ACESSO: a capacidade de um usuário de executar uma tarefa específica, como exibir, criar ou alterar um arquivo ou acessar determinadas telas e informações dentro de um sistema;

II – ACESSO IMOTIVADO: aquele realizado para fins estranhos às tarefas funcionais do usuário;

III – ATIVOS DE INFORMAÇÃO: os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;

IV – AUTENTICIDADE: garante a identidade de quem envia a informação e a veracidade da fonte da informação;

V – COLABORADORES: empregados, estagiários, servidores cedidos à RS-Prev, contratados e aprendizes;

VI – CONTA DE USUÁRIO: conjunto de direitos e propriedades de um usuário que provê acesso a recursos de um sistema;

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

VIII – DIRIGENTES: Conselheiros Fiscais e Deliberativos e, quando implantados, membros dos Órgãos Auxiliares definidos no Estatuto da RS-Prev;

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

X – GESTÃO DA INFORMAÇÃO: diz respeito ao ciclo de atividade organizacional desde 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;

XI – GESTORES: Diretores Executivos e gerentes da RS-Prev;

XII – INCIDENTE DE SEGURANÇA DA INFORMAÇÃO: qualquer indício de fraude, sabotagem, espionagem, desvio, falha ou evento indesejado ou inesperado que tenha probabilidade de comprometer ou ameaçar a segurança da informação;

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

XIV – INFORMAÇÕES CUSTODIADAS: informações sob a responsabilidade da RS-Prev cedidas pelo seu proprietário em razão de contrato, acordo, convênio ou ajuste;

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

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

XVII - PARCEIROS DE NEGÓCIOS: bancos comerciais e de investimentos, prestadores de serviço de gestão dos recursos financeiros, gestão do passivo, gestão dos benefícios programados e não programados e a oferta dos planos a potenciais participantes, inclusive serviços de auditoria independente, de seguro ou resseguro, de comunicação social e de tecnologia da informação que estejam diretamente vinculados à operação dos planos de benefícios e outros prestadores de serviços que atuam junto à RS-Prev;

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

XIX – *PHISHING SCAM*: tentativa de fraude pela que utiliza "iscas", artifícios para atrair a atenção de uma pessoa e fazê-la realizar alguma ação;

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

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

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

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

XXIV – *SPAM*: mensagem eletrônica não solicitada;

XXV – TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO: conjunto de recursos tecnológicos integrados, os quais proporcionam, por meio das funções de hardware, software e telecomunicações, a automação e comunicação de processos;

XXVI – TERMO DE RESPONSABILIDADE DE ACESSO: instrumento a ser assinado por todos usuários, em que dão ciência sobre as diretrizes desta Política e se responsabilizam pelo acesso e uso dos recursos computacionais da RS-Prev;

XXVII – USUÁRIO: pessoa que utiliza bem ou serviço da RS-Prev, por meio de ferramentas ou dispositivos para se comunicar com os outros, escrever, disponibilizar ou publicar documentos; e

XXVIII – VIOLAÇÃO DA SEGURANÇA DA INFORMAÇÃO: qualquer fraude, sabotagem, espionagem, desvio, falha ou evento indesejado ou inesperado que tenha probabilidade de comprometer ou ameaçar a segurança da informação.

3. OBJETIVOS

3.1. Esta Política, propõe-se a estabelecer o conjunto de diretrizes e princípios que norteiam as medidas de proteção das informações geradas ou custodiadas pela RS-Prev,

para minimizar os riscos de falhas, danos, acessos imotivados ou prejuízos que possam comprometer a continuidade do fluxo de informações.

3.2. Os principais objetivos da PGSI são:

I - Proteger as informações custodiadas pela RS-Prev, preservando a confidencialidade, integridade, disponibilidade, autenticidade, legalidade e o sigilo;

II - Estabelecer diretrizes relacionadas à segurança da informação, envolvendo o tratamento de dados e informações da RS-Prev;

III - Prevenir eventuais interrupções, totais ou parciais, dos serviços de Tecnologia da Informação e Comunicação - TIC da RS-Prev e, no caso de sua ocorrência, reduzir os impactos delas resultantes; e

IV – Prevenir e prever o tratamento de incidentes de segurança da informação no âmbito da RS-Prev.

4. ABRANGÊNCIA

4.1. As disposições desta Política aplicam-se a todos os colaboradores, gestores, dirigentes, prestadores de serviços, fornecedores e parceiros de negócios que tenham acesso a informações e documentos, bem como ao ambiente de tecnologia da informação da RS-Prev.

5. PRINCÍPIOS

5.1. Nesta Política as ações relacionadas com a gestão e segurança da informação serão norteadas pelos seguintes princípios:

I – CELERIDADE: oferecer respostas rápidas a incidentes e falhas de gestão e segurança da informação;

II – CLAREZA: as regras, documentações e comunicações devem ser precisas, concisas e de fácil entendimento;

III – CONFIDENCIALIDADE: princípio de segurança que estabelece restrições ao acesso e à utilização da informação;

IV – CONFIABILIDADE: garantir o armazenamento e proteção das informações, tornando-as acessíveis apenas aos autorizados a acessá-las;

V – DISPONIBILIDADE: princípio que garante que os usuários autorizados tenham acesso à informação e aos ativos correspondentes sempre que necessário;

VI – INTEGRIDADE: garantia que a informação tenha suas características originais resguardadas;

VII – TRANSPARÊNCIA: assegurar uma gestão transparente da informação, por meio de medidas efetivas que proporcionem o acesso e sua divulgação de acordo com a legislação vigente; e

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

6. DIRETRIZES GERAIS

6.1. A informação produzida ou custodiada pela RS-Prev deve ser preservada de acordo com as necessidades específicas do serviço, alinhadas aos requisitos legais e exigências dos órgãos reguladores e fiscalizadores;

6.2. Todo equipamento fornecido pela empresa deve ser utilizado para a realização das tarefas profissionais dos colaboradores, podendo ser utilizado em questões particulares dentro de critérios da razoabilidade e responsabilidade;

6.3. A internet fornecida pode ser utilizada pelos colaboradores para fins pessoais, desde que não prejudique o rendimento do trabalho prestado à instituição;

6.4. Não será permitido armazenar, transmitir ou compartilhar conteúdo indevido ou ilegal nos ativos de propriedade e responsabilidade da RS-Prev;

6.5. Esta Política deve ser comunicada a todos os colaboradores, dirigentes e gestores, para que seja seguida dentro e fora do ambiente corporativo, nas atividades inerentes à RS-Prev;

6.6. Qualquer incidente que possa vir a acontecer e que afete os quesitos da segurança da informação deve ser informado à Área de TIC da RS-Prev, que tomará as devidas medidas para a correção;

6.7. As senhas de acesso são individuais, intransferíveis, de responsabilidade única e exclusiva do usuário e não podem ser compartilhadas ou divulgadas; e

6.8. Esta Política será implementada por meio de procedimentos específicos, e será de obrigatoriedade de todos os colaboradores o seu seguimento, independentemente de cargo, função, serviços prestados e níveis hierárquicos.

7. REGRAS E DIRETRIZES ESPECÍFICAS

7.1. Credenciais de acesso

7.1.1. As credenciais de acesso, compostas por conta de usuário e senha, serão fornecidas pela Área de TIC, mediante a solicitação escrita da Diretoria demandante, por meio eletrônico;

7.1.2. As contas de usuário e senha seguirão o padrão adotado pela Área de TIC e serão pessoais e intransferíveis;

7.1.2.1. Os usuários poderão alterar a própria senha, e devem ser orientados a fazê-lo, caso suspeitem que terceiros obtiveram acesso indevido ao seu *login*/senha. A periodicidade máxima para troca das senhas é 180 (cento e oitenta) dias, não podendo ser repetidas as 2 (duas) últimas senhas, e possuindo complexidade.

7.1.3. Estas credenciais de acesso definem os direitos de acesso de cada usuário, de acordo com o cargo ocupado e função desempenhada;

7.1.4. As permissões de acesso deverão respeitar a segregação de funções, hierarquia de atividades, cargos ou funções, com vistas a evitar que ocorram acessos conflitantes e cumulativos, bem como mitigar a possibilidade de eventuais riscos de segurança operacional, financeiro e de fraude;

7.1.5. Os acessos às informações e a utilização dos recursos corporativos poderão ser monitorados;

7.1.6. Todo acesso realizado em um determinado sistema deverá ser registrado e armazenado de forma segura e protegida, para fins de auditoria, quando permitido pelo sistema;

7.1.7. Devem ser realizadas revisões de acesso a fim de garantir a desabilitação de usuários indevidos, a revisão das permissões concedidas, a existência de perfis de acesso com privilégios maiores do que o necessário para execução das atividades;

7.1.8. Os colaboradores devem bloquear suas estações de trabalho quando da ausência de seu posto; e

7.1.9. A instalação de qualquer recurso, seja *software* ou *hardware*, será de responsabilidade da Área de TIC.

7.2. Recursos Computacionais e Tecnologias

7.2.1 O usuário da informação, independentemente do cargo ocupado ou da área em que esteja alocado, não deve:

I – Abrir ou manusear com fins de reparo qualquer ativo de TIC pertencente à RS-Prev;

II – Alterar configurações, em especial referentes à segurança da informação, acessos e registros realizados;

III – Desinstalar programas, aplicativos, recursos, *plugins*, sem a devida autorização e acompanhamento da Área de TIC da RS-Prev;

IV – Remover das dependências da RS-Prev qualquer ativo de TIC, sem a devida autorização da Área de TIC ou gestor imediato;

V – Acessar, visualizar, baixar (efetuar *download*), instalar, armazenar, divulgar, repassar, subir (efetuar *upload*) e transpor para mídias físicas (imprimir ou gravar em outras mídias móveis) qualquer material, conteúdo, serviço ou recurso:

a. Que desrespeite os direitos de propriedade intelectual da RS-Prev ou de terceiros;

b. Com fins de propaganda política; e

c. Programas aplicativos, recursos, ferramentas, arquivos e *plugins* de origem duvidosa ou não homologados previamente pela Área de TIC da RS-Prev.

VI – Efetuar acesso imotivado; e

VII – Utilizar ativos de propriedade particular com a finalidade de burlar as restrições estabelecidas nesta Política.

7.2.2. Quando ocorrer o desligamento do usuário, as informações armazenadas nos ativos em sua posse devem ser analisadas pelo seu gestor imediato, para que este determine quem será o novo responsável pelo manuseio das informações.

7.3. Trabalho Remoto e Dispositivos Móveis

7.3.1. A concessão de acesso remoto deve ser realizada de modo a atender às atividades da RS-Prev e limitada às atribuições, cargo ou funções do usuário;

7.3.2. Esta concessão de acesso remoto deve ser solicitada pelo usuário ao seu gestor imediato, podendo ser revogada a qualquer tempo e sem aviso prévio;

7.3.3. Será instalado em sua máquina um *software* de acesso remoto;

7.3.4. O usuário deve utilizar os serviços de acesso remoto em ambientes seguros de conexão;

7.3.5. Os usuários estão cientes de que a Área de TIC pode monitorar todos os acessos e usos de suas informações, bem como de seus ambientes, com a finalidade de cumprimento desta Política;

7.3.6. O usuário que utiliza os recursos de acesso remoto ao ambiente corporativo da RS-Prev deve proteger suas credenciais de acessos e realizar o encerramento da sessão ao término de suas atividades;

7.3.7. É vedado ao usuário a cópia de arquivos e documentos de propriedade da RS-Prev para os dispositivos particulares sem a prévia autorização do gestor imediato, salvo os publicados na internet;

7.3.8. A utilização dos dispositivos móveis deve ser realizada com a finalidade de atender às atividades da RS-Prev, limitada às atribuições, cargo ou funções do usuário;

7.3.9. A instalação e configuração dos dispositivos móveis somente será realizada pela Área de TIC;

7.3.10. O usuário deve informar imediatamente à Área de TIC, quando da ocorrência de qualquer avaria, dano ou defeito do dispositivo de mobilidade pertencente à RS-Prev;

7.3.11. No caso da ocorrência de perda, furto ou roubo de dispositivo de propriedade da RS-Prev, o usuário deve comunicar imediatamente à Área de TIC e registrar um Boletim de Ocorrência;

7.3.12. Os dispositivos móveis pessoais que não fazem parte dos ativos da RS-Prev, só devem ser conectados à rede corporativa por meio da rede sem fios através de acesso obtido junto à Área de TIC.

7.4. Correio Eletrônico

7.4.1. A utilização de correio eletrônico corporativo é restrita às atividades profissionais do usuário;

7.4.2. O endereço de correio eletrônico corporativo e o conteúdo das caixas postais disponibilizadas aos usuários são de propriedade da RS-Prev;

7.4.3. Será concedido de forma automática aos usuários o acesso remoto ao *e-mail* corporativo;

7.4.4. O acesso à caixa postal corporativa é realizado por meio de senha, de caráter pessoal e intransferível, sendo vedado ao usuário fornecê-la a terceiros ou ser negligente quanto a sua guarda;

7.4.5. O *e-mail* corporativo possui um limite pré-definido para o armazenamento das mensagens, devendo o usuário efetuar, periodicamente, a limpeza de sua caixa postal corporativa, excluindo mensagens desnecessárias, para não exceder o limite de armazenamento.

7.4.5.1. O usuário poderá solicitar auxílio à Área de TIC, para proceder a gestão e arquivamento das mensagens, com o propósito de garantir o *backup* das informações relevantes;

7.4.6. O usuário poderá realizar a sincronização com seu respectivo *e-mail* corporativo em seus dispositivos pessoais, somente após a autorização do seu gestor imediato;

7.4.7. É vedado aos usuários:

I – Enviar mensagens cujo conteúdo possa gerar, de forma direta ou indireta, riscos a imagem da RS-Prev;

II – Enviar mensagem a partir de endereço de e-*mail* corporativo diferente do seu, ou que não esteja autorizado a usar ou se fazer passar por outra pessoa;

III – Abrir mensagens consideradas suspeitas ou caracterizadas como *spam* e *phishing scam*;

IV – Produzir, armazenar, transmitir ou divulgar mensagens que não sejam compatíveis com esta Política, bem como a missão, visão e valores, que sejam ofensivas à RS-Prev ou à terceiros, ou que caracterizem invasão de privacidade; e

V – Constituir violação de direitos de propriedade intelectual da RS-Prev ou de terceiros.

7.5. Uso da Internet

7.5.1. O acesso à Internet da RS-Prev é destinado às finalidades profissionais e restritas do usuário, podendo ser utilizado para fins pessoais dentro de critérios de razoabilidade e responsabilidade;

7.5.2. Os Termos e Condições de Uso e a Política de Privacidade dos sites acessados na internet devem ser lidos antes de qualquer inscrição ou atividade, quando aplicável;

7.5.3. Não é permitido visualizar, utilizar, armazenar, divulgar, repassar e imprimir qualquer material, conteúdo, serviço ou recurso que não seja compatível com as atividades da RS-Prev, como por exemplo:

I – Arquivos executáveis, com a extensão ".exe", ou equivalentes, não autorizados pela Área de TIC;

II – Sites contendo pornografia, pedofilia, incitação ao terrorismo ou qualquer outro conteúdo que atente contra as leis vigentes e a ordem pública;

III – Jogos *on-line* ou *off-line*;

IV – Programas de compartilhamento de arquivos e de comunicação instantânea não autorizados pela Área de TIC; e

V – Programas ou *plugins* de camuflagem de navegação, deleção de histórico de navegação.

7.5.4. Não é permitido efetuar o *upload* indevido de qualquer conteúdo de propriedade da RS-Prev;

7.5.5. Não é permitido acessar indevidamente dados, sistemas ou redes, incluindo qualquer tentativa de investigar, examinar ou testar vulnerabilidades em sistemas internos ou externos da RS-Prev;

7.5.6. Tentar indevidamente obstruir, desativar ou alterar os controles de segurança e os seus parâmetros estabelecidos nos ativos pela Área de TIC; e

7.5.7. Tentar interferir em um serviço, sobrecarregá-lo ou desativá-lo, inclusive aderir ou cooperar com ataques de negação de serviços internos ou externos da RS-Prev.

7.6. Mídias Sociais

7.6.1. O acesso e uso de mídias sociais particulares a partir da conexão corporativa da RS-Prev é passível de restrição em caso de uso indevido ou fora dos critérios de razoabilidade que norteiam o trabalho de cada área;

7.6.2. As áreas ou usuários que possuem o acesso corporativo autorizado às mídias sociais da RS-Prev devem fazer o seu uso apenas no âmbito de suas competências e atividades profissionais determinadas;

7.6.3. Os usuários que não possuem o acesso corporativo autorizado às mídias sociais, mas que com elas interagem por meio dos ativos da RS-Prev, não devem:

I – Publicar qualquer conteúdo ou opinião nas mídias sociais em nome da RS-Prev;

II – Publicar qualquer conteúdo sobre a RS-Prev, seus clientes, seus parceiros, seus fornecedores e colaboradores, com exceção das informações públicas;

III – Publicar conteúdos audiovisuais, como fotos, imagens, vídeos ou áudios relacionados ao âmbito interno da RS-Prev tais como, instalações físicas, ambientes e equipes, caso exista o risco de vazamento de informações não-pública;

IV – Publicar assuntos profissionais internos ou específicos da RS-Prev ligados à atividade exercida ou que esteja protegida por sigilo profissional; e

V – Publicar conteúdo de cunho político, religioso, de gênero, raça ou qualquer outro que viole a privacidade de outrem nas relações de trabalho, ou implique na imagem da RS-Prev.

7.7. Telefonia

7.7.1. Todo usuário é responsável pelas ligações efetuadas a partir de seu ramal dentro do seu horário de expediente, sendo que ligações de caráter pessoal, ainda que permitidas, poderão ser cobradas;

7.7.2. Os colaboradores da RS-Prev estão cientes de que todas as ligações efetuadas através do sistema de telefonia da RS-Prev são passíveis de gravação, considerando que o sistema de telefonia se destina ao uso em serviço.

8. RESPONSABILIDADES

8.1. Da Diretoria de Administração

8.1.1. Analisar criticamente e de forma periódica esta Política e os demais normativos a ela relacionados, avaliando se continua alinhada aos requisitos das atividades da RS-Prev e propondo eventual revisão à Diretoria-Executiva;

8.1.2. Designar formalmente os responsáveis pela gestão de acesso, bem como monitorar e assegurar que as melhores práticas relativas à gestão de acessos sejam adotadas e praticadas;

8.1.3. Orientar e conscientizar os usuários da RS-Prev a respeito desta Política;

8.1.4. Gerenciar as permissões de acesso respeitando a hierarquia de atividades, cargos ou funções, evitando que ocorram acessos conflitantes e cumulativos, bem como mitigar a possibilidade de eventuais riscos operacionais, financeiros e de fraudes; e

8.1.5. Controlar os contratos firmados com terceiros e incluir cláusulas de confidencialidade, de acesso e tratamento de dados, em cumprimento à todas as regras definidas nesta Política, nos normativos que tratam de segurança de dados e demais normas internas.

8.2. Dos demais gestores

8.2.1. Apontar os acessos conflitantes e cumulativos, que podem incorrer em riscos e solicitar sua devida adequação;

8.2.2. Revisar as permissões concedidas aos usuários de sua equipe, bem como mantê-los cientes das regras estabelecidas nesta Política.

8.3. Dos usuários

8.3.1. Cumprir esta Política e os demais documentos regulamentares relacionados a ela, de forma responsável, profissional, ética e legal;

8.3.2. Todo usuário é responsável pela proteção das informações da RS-Prev, conforme a Lei 13.709/2018 (Lei Geral de Proteção de Dados – LGPD) e demais normativos internos;

8.3.3. Buscar orientação da Área de TIC em caso de dúvidas relacionadas à Segurança da Informação;

8.3.4. Comunicar ao gestor imediato ou à Área de TIC qualquer irregularidade ou desvio de regras desta Política;

8.3.5. Utilizar apenas programas, aplicativos, recursos, ferramentas ou *plugins* homologados para uso pela Área de TIC, sejam eles gratuitos, livres ou licenciados;

8.3.6. Todo usuário ao receber ou utilizar um ativo deve verificar o estado de conservação em que este se encontra, sendo o responsável por zelar pelo estado de conservação do ativo; e

8.3.7. Para acessar os aplicativos corporativos disponibilizados pela RS-Prev, o usuário deverá estar identificado, autenticado e autorizado. Os acessos serão concedidos à medida que solicitados e autorizados pelo gestor imediato.

8.4. Área de TIC

8.4.1. Propor normas, procedimentos, planos e processos para a operacionalização desta política, sugerindo melhorias quando necessário;

8.4.2. Realizar ações preventivas e educativas quando aos dispositivos desta Política;

8.4.3. Disseminar a cultura da segurança da informação no âmbito da RS-Prev;

8.4.4. Propor a realização de análise de riscos e mapeamento de vulnerabilidades nos ativos;

8.4.5. Registrar todas as alterações e configurações dos ativos de infraestrutura e servidores da RS-Prev;

8.4.6. Realizar todo e qualquer processo de manutenção, instalação, configuração, desinstalação, substituição ou remanejamento de qualquer ativo na RS-Prev, sendo responsável pela guarda de suportes físicos (mídias); e

8.4.7. Ser responsável pela gestão dos ativos de infraestrutura e servidores da RS-Prev.

9. PENALIDADES

9.1. O descumprimento das disposições constantes nesta Política e nas normas e políticas complementares, caracteriza infração funcional, a ser apurada em procedimento administrativo disciplinar e civil, sem prejuízo da responsabilidade penal.

10. REFERÊNCIAS

10.1. Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais - LGPD;

10.2. Resolução CGPC nº 13, de 1º de outubro de 2004: Estabelece princípios, regras e práticas de governança, gestão e controles internos a serem observados pelas Entidades Fechadas de Previdência Complementar – EFPC;

10.3. Norma NBR ISO/IEC 27001:2013: Tecnologia da Informação – Técnicas de Segurança – Define os requisitos e diretrizes dos Sistemas de gestão da segurança da informação – SGSI;

10.4. Norma NBR ISO/IEC 27002:2013: Tecnologia da Informação – Técnicas de Segurança – Código de prática para a gestão da segurança da informação;

10.5. Política de Privacidade e Proteção de Dados Pessoais da RS-Prev.

11. DISPOSIÇÕES FINAIS

11.2. A revisão desta Política será realizada observando a legislação vigente, bem como os critérios definidos nos normativos internos da RS-Prev, cabendo ao usuário manter-se atualizado quanto às disposições deste documento;

11.4. A íntegra desta Política deverá ficar disponível no sítio eletrônico da RS-Prev.