POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

"POSIC"

Dezembro de 2018

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

Histórico de alterações e atualizações

Data	Versão	Criado por	Descrição da alteração
26/11/2018	0.1	Marcelo Mendonça	Layout e Estruturação da POSIC.
03/12/2018	0.2	Marcelo Mendonça	Primeira versão da POSIC finalizada.

Histórico de revisões

Data	Revisado por	Seções revisadas
09/12/2018	Jordan Melo	Todas

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

SUMÁRIO

1 INTRODUÇÃO

A Amapá Previdência – AMPREV é a Unidade Gestora do Sistema Próprio de Previdência Social dos servidores públicos civis e militares, ativos, inativos e pensionistas do Estado do Amapá. Devido à natureza de suas atividades, a informação utilizada pelo órgão é um bem que tem valor significativo para sociedade. Por esta razão, a informação deve ser protegida e gerenciada adequadamente com o objetivo de garantir sua disponibilidade, integridade, confidencialidade e autenticidade.

Para assegurar o cumprimento dos objetivos de negócio e a missão social da Amapá Previdência é fundamental que seja desenvolvida e implantada uma Política de Segurança da Informação e Comunicações, que vise combater as ameaças aos ativos de informação, bem como conscientizar os usuários, servidores, colaboradores, clientes, parceiros e fornecedores para a utilização correta e segura dos recursos de Tecnologia da Informação oferecidos pelo órgão.

2 CONCEITOS E DEFINIÇÕES

Para efeitos desta Política, entende-se:

I. **Informação**: todo e qualquer conteúdo que possua valor agregado para a organização, podendo ser apresentado nas mais diversas formas, como impressa, escrita, falada, filmada, ou gravada em dispositivos eletrônicos ou magnéticos como CDs, DVDs, disquetes, discos de armazenamento, pen drives, estações de trabalho e qualquer outro meio existente.

II. **Ativos de informação**: meios de armazenamento, transmissão e processamento da informação, bem como os equipamentos necessários, os sistemas utilizados, os locais onde se encontram esses meios, e também os recursos humanos que a eles têm acesso.

III. **Ameaça**: conjunto de fatores internos e externos ou causa potencial de um incidente, que pode resultar em dano para um sistema ou organização.

IV. **Incidente de Segurança da Informação e Comunicações**: gerado por um ou mais eventos indesejados ou inesperados, que tenham probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação.

V. **Disponibilidade**: garantia de que a informação esteja acessível e utilizável por uma pessoa física ou determinado sistema, órgão ou entidade.

VI. **Integridade**: garantia de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental. Salvaguarda da exatidão e completeza da informação e dos métodos de processamento.

VII. **Confidencialidade**: garantia de que a informação não seja disponibilizada ou revelada à pessoa física, sistema, órgão ou entidade que não possuam o devido credenciamento e permissão para tal acesso.

VIII. **Autenticidade**: garantia de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade.

IX. **Riscos de Segurança da Informação e Comunicações**: potencial vinculado à exploração de uma ou mais vulnerabilidades de um ou mais ativos de informação, por parte de uma ou mais ameaças, com impacto negativo sobre o negócio.

X. **Continuidade de Negócios**: capacidade estratégica de uma organização se planejar e responder a incidentes e interrupções de negócios, minimizando seus impactos e recuperando perdas de ativos de informação, mantendo as operações críticas em um nível aceitável de funcionamento.

XI. **Usuários**: Empregados, técnicos, analistas, diretores, conselheiros, cargos, requisitados e cedidos, desde que previamente autorizados, empregados de empresas prestadoras de serviços terceirizados, consultores, estagiários, e outras pessoas que se encontrem a serviço da Amapá Previdência.

3 OBJETIVOS

A Política de Segurança da Informação e Comunicações da Amapá Previdência tem como objetivos:

I. Prover orientação da Direção e apoio para a segurança da informação e comunicações de acordo com os requisitos do negócio e com as leis e regulamentações relevantes.

II. Estabelecer diretrizes estratégicas que orientem e apoiem as ações organizacionais, visando preservar, em qualquer meio, a confidencialidade, integridade, disponibilidade e autenticidade da informação.

III. Promover práticas de segurança da informação e comunicações, compatíveis com o uso aceitável das informações e dos ativos que as mantém, minimizando os riscos sobre o negócio.

IV. Prover mecanismos de transparência e gestão das informações.

V. Contribuir para o cumprimento da missão da Amapá Previdência e a melhoria contínua dos resultados institucionais em prol da sociedade.

4 ABRANGÊNCIA

As diretrizes estabelecidas por esta Política aplicam-se a:

I. Todos os ambientes físicos pertencentes ao patrimônio da Amapá Previdência ou sob sua custódia.
II. Todos os ambientes computacionais e ativos de informação pertencentes a Amapá Previdência.
III. Todos os contratos, convênios, acordos, termos e outros instrumentos congêneres celebrados pela Amapá Previdência.
IV. Todos os empregados, técnicos, analistas, diretores, conselheiros, cargos, requisitados e cedidos, empregados de empresas prestadoras de serviços terceirizados, consultores, estagiários, e outras pessoas que se encontrem a serviço da Amapá Previdência.

Esta Política conscientiza cada colaborador de que os ambientes, sistemas, computadores e redes da AMPREV poderão ser monitorados e gravados, conforme previsto nas legislações do País.

É mandatório que cada colaborador se mantenha atualizado em relação às diretrizes, procedimentos e normas relacionadas a esta Política, buscando orientação sempre que não estiver seguro quanto aos itens aqui propostos.

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

5 PRINCÍPIOS

Os princípios básicos norteadores desta Política de Segurança da Informação e Comunicações são:

I. A segurança dos colaboradores e da vida humana tem precedência sobre qualquer ativo da Amapá Previdência.
II. Preservar a reputação da Amapá Previdência e de seus colaboradores.
III. Zelar pela proteção do direito individual e coletivo das pessoas, relacionado à inviolabilidade de sua intimidade.

IV. Garantir a proibição de acesso, uso, guarda e encaminhamento de material antiético, discriminatório, malicioso, obsceno ou ilegal.
V. Toda informação produzida ou adquirida como resultado das atividades do negócio pertence a Amapá Previdência.
VI. Deverá haver, em todos os contratos da Amapá Previdência, cláusula de confidencialidade, como condição exigida para autorização de acesso aos ativos de informação disponibilizados pelo órgão.
VII. O nível de complexidade e os custos das ações de segurança da informação e comunicações devem ser proporcionais ao valor dos ativos e informações.
VIII. Zelar pela transparência das informações públicas, observando os critérios de legalidade.
IX. Possibilitar o acesso à informação por pessoas portadoras de necessidades especiais.
X. Zelar pela economia e conservação dos bens e recursos da Amapá Previdência.
XI. Conscientizar os colaboradores sobre as diretrizes e procedimentos de segurança, possibilitando o uso correto dos recursos e reduzindo riscos.
XII. Garantir que as ações de segurança da informação e comunicações sejam alinhadas com os objetivos de negócio da Amapá Previdência.
XIII. Garantir que a segurança da informação e comunicações esteja efetivamente incorporada no desempenho das atividades realizadas pelo órgão.

Além dos princípios acima expostos, deverão ser considerados os princípios fundamentais que regem a Administração Pública Federal, contidos na Constituição Federal do Brasil.

6 DIRETRIZES

Nesta seção serão elencadas as diretrizes gerais e específicas da Política de Segurança da Informação e Comunicações da Amapá Previdência.

6.1 Gestão de ativos

Objetivos: Identificar os ativos da organização e definir as devidas responsabilidades pela proteção dos mesmos. Assegurar que a informação receba um nível adequado de proteção, de acordo com a sua importância para a organização. Prevenir a divulgação não autorizada, modificação, remoção ou destruição da informação armazenada nas mídias.

Diretrizes:

I. Os ativos associados à informação e aos recursos de processamento da informação devem ser identificados, estruturados e inventariados.

II. Os ativos devem ser classificados de acordo com sua importância ou criticidade, para que se possa estabelecer métodos de processamento, armazenamento, transmissão, exclusão e destruição da informação por eles suportada.

III. Todos os ativos inventariados devem possuir um responsável ou proprietário.

IV. Os responsáveis pelos ativos devem ser definidos pela alta direção da Amapá Previdência.

V. O responsável designado pode ser um indivíduo ou uma entidade que aprovou a responsabilidade pela gestão, para controlar todo o ciclo de vida de um ativo.

VI. Todos os colaboradores e terceiros que usam ou têm acesso aos ativos de informação da AMPREV devem estar cientes dos requisitos de segurança da informação destes ativos.

VII. Todos os colaboradores e partes externas devem devolver todos os ativos da organização que estejam em sua posse, após o encerramento de suas atividades, do contrato ou acordo.

VIII. Toda informação gerada na Amapá Previdência deve ser classificada em termos do seu valor, requisitos legais, sensibilidade e criticidade para evitar modificação ou divulgação não autorizada.

IX. O nível de proteção deve ser avaliado por meio da análise de confidencialidade, integridade, disponibilidade e autenticidade.

X. Para cada nível de proteção deve ser dado um nome que faça sentido dentro do esquema de classificação.

XI. Devem ser estabelecidos procedimentos para o tratamento, processamento, armazenamento e transmissão da informação, de acordo com sua classificação. Para tanto, consideram-se os seguintes itens:

    a. Restrições de acesso baseadas no nível de classificação.
    b. Proteção de cópias temporárias ou permanentes da informação.
    c. Armazenamento dos ativos de TI de acordo com as especificações dos fabricantes.

XII. Toda mídia deve ser guardada de forma segura em ambiente protegido, de acordo com o nível de classificação da informação nela contida.

XIII. Quando a informação contida na mídia for confidencial, técnicas de criptografia devem ser adotadas para aumentar a proteção dos dados.

XIV. Em caso de falhas em mídias, decorrentes de degradação natural ou mau uso dos dispositivos, realizar a transferência das informações críticas para novas mídias de armazenamento.

XV. Informações valiosas devem ser armazenadas em mídias separadas, para minimizar os riscos futuros de perda ou dano de mídias.

XVI. Mídias contendo informações sigilosas devem ser guardadas e destruídas de forma segura e protegida. Dependendo da informação contida, procedimentos como incineração ou trituração devem ser adotados.

XVII. Os itens que demandam descarte seguro devem ser previamente detectados.

XVIII. Em casos complexos, estudar a viabilidade de contratação de um fornecedor bem reputado, que apresente controles seguros e adequados para o descarte de mídias.

XIX. O descarte de itens sensíveis deve ser registrado, sempre que possível, para manutenção de uma trilha de auditoria.

6.2 Controle de acesso

Objetivos: Limitar o acesso à informação e aos recursos de processamento da informação. Garantir o acesso aos usuários autorizados e restringir aos não autorizados.

Diretrizes:

I. Estabelecer requisitos formais para criação, inativação e remoção de usuários de acesso.
II. Estabelecer requisitos para autorização e desautorização formal de acesso aos sistemas da Amapá Previdência.
III. Registrar em arquivos de log todos os eventos significativos, relativos ao uso e gerenciamento dos sistemas, detectando a identidade do usuário e suas ações realizadas.
IV. Estabelecer regras de acesso privilegiado.
V. Definir regra padrão de “Tudo proibido” e criar liberações excepcionais caso a caso.
VI. Evitar utilização de usuário administrador para não comprometer processos de auditoria.
VII. Estabelecer procedimentos de autorização para determinar quem tem permissão para acessar quais redes e serviços de redes.
VIII. Definir meios seguros de acesso às redes da Amapá Previdência, utilizando protocolos que utilizem criptografia como SSH, SFTP, VPN IPSEC, dentre outros.
IX. Não utilizar protocolos inseguros como FTP, TELNET e quaisquer outros que não utilizem algoritmos de criptografia associados a métodos de autenticação.
X. Criar mecanismos para realizar monitoramento da disponibilidade e do uso dos serviços de rede.
XI. Todos os colaboradores e usuários devem manter a confidencialidade da informação de autenticação secreta, não fornecendo suas credenciais de acesso para outras partes, incluindo autoridades e lideranças.
XII. Os direitos de acesso dos usuários devem ser revisados e ajustados regularmente ou sempre que houver quaisquer mudanças, como promoção, remanejamento ou encerramento de contrato.
XIII. Os usuários devem evitar manter anotada a informação de autenticação secreta (por exemplo, papel, arquivos ou dispositivos móveis), a menos que ela possa ser armazenada de forma segura e o método de armazenamento esteja aprovado, como em um sistema de gerenciamento de senhas, por exemplo.
XIV. Os usuários devem requisitar ou alterar suas senhas, sempre que existir qualquer indicação de possível comprometimento do sistema ou da própria senha.
XV. Definir quais informações podem ser acessadas por cada usuário em particular e controlar os direitos de acesso com permissões, como, ler, escrever, excluir e executar.
XVI. Prover controles de acesso lógico ou físico como método de isolamento de aplicações, dados ou sistemas críticos.

XVII. Em sistemas que requerem verificação de identidade e autenticação forte, utilizar métodos alternativos de autenticação para as senhas, como meios criptográficos, *smart cards*, *tokens* ou biometria.

XVIII. Registrar, sempre que possível, as tentativas forçadas de acesso aos sistemas.

XIX. Registrar, sempre que possível, as tentativas de acesso mal e bem sucedidas aos sistemas.

XX. Garantir que as senhas não sejam transmitidas em texto claro pela rede.

XXI. As informações de autenticação secreta devem possuir requisitos de complexidade para evitar senhas fracas facilmente identificadas por ataques de dicionário.

XXII. Prover meios de controlar e impedir a utilização de programas utilitários privilegiados, utilizados para sobrepor e reduzir o nível de segurança da rede e dos sistemas.

6.3 Controles criptográficos

Objetivos: Assegurar o uso efetivo e adequado da criptografia para proteger a confidencialidade, autenticidade e integridade da informação.

Diretrizes:

I. Identificar o nível de proteção exigido pelos ativos, levando em consideração uma avaliação de risco, para que seja possível definir a força e a qualidade do algoritmo de criptografia requerido.

II. Utilizar criptografia para proteger as informações críticas transportadas em dispositivos móveis, mídias removíveis ou através de redes de computadores.

III. Utilizar certificados SSL assinados por autoridades certificadoras confiáveis em sistemas web, para garantir que as informações acessadas ou transmitidas não sejam interceptadas por pessoas não autorizadas.

IV. Utilizar assinaturas digitais ou códigos de autenticação para validar a autenticidade ou integridade de informações críticas armazenadas ou transmitidas.

V. Os algoritmos criptográficos e o tamanho de chaves devem ser selecionados de acordo com o nível de criticidade das informações e dos sistemas que a suportam, para que não ocorram impactos desnecessários tanto de falta de segurança, quanto de segurança excessiva (por exemplo, causando lentidão demasiada no acesso a informações simples e pouco críticas).

VI. Todas as chaves criptográficas devem ser protegidas contra modificação e perda.

VII. As chaves privadas e secretas devem ser protegidas contra uso ou divulgação não autorizada.

VIII. As chaves devem ser distribuídas de forma segura para os usuários devidamente autorizados.

IX. Revogar chaves comprometidas ou àquelas utilizadas por usuários que não possuírem mais autorização para tal utilização.

6.4 Segurança física e do ambiente

Objetivos: Prevenir o acesso físico não autorizado, danos e interferências nos recursos de processamento das informações e nas informações da organização.

Diretrizes:

I. Definir os perímetros de segurança e garantir que a localização e capacidade de resistência de cada perímetro dependam dos requisitos de segurança dos ativos existentes no interior do perímetro.
II. Os perímetros que contenham instalações de processamento da informação devem ser fisicamente sólidos, sem brechas ou pontos que facilitem ações de invasão. Além disso, as portas externas devem possuir construção robusta e protegida adequadamente contra acessos não autorizados.
III. Implantar área de recepção, ou outro meio que possibilite o controle de acesso físico ao edifício da AMPREV.
IV. Registrar a data e hora de entrada e saída de visitantes, bem como supervisionar a permanência dos mesmos nos interiores do prédio.
V. Garantir que somente pessoas autorizadas tenham acesso às áreas em que são processadas informações sensíveis.
VI. Prestadores de serviço terceirizado somente terão acesso às áreas seguras de processamento da informação, quando for requisitado pela Amapá Previdência e for realmente necessário.
VII. Escritórios, salas e instalações-chave devem ser localizados de modo a evitar o acesso do público.
VIII. As áreas seguras, não ocupadas, devem ser fisicamente trancadas e periodicamente verificadas.
IX. Proibir atos de comer, beber e fumar nas proximidades das instalações de processamento da informação.
X. Garantir condições ambientais adequadas, como temperatura e umidade, para evitar prejuízos nas instalações de processamento da informação.
XI. Proteger os equipamentos que suportam informações críticas, contra falta de energia elétrica e outras interrupções.
XII. Impedir que os equipamentos, informações ou *softwares* sejam retirados das dependências da AMPREV sem autorização prévia.
XIII. Realizar registro da retirada e devolução de ativos das dependências da Amapá Previdência.

6.5 Tópicos relacionados aos usuários

Objetivos: Garantir o uso aceitável dos recursos da Amapá Previdência por parte dos usuários, adotando medidas e bons hábitos em segurança da informação e comunicações, prevenindo eventos indesejados que gerem impactos sobre o negócio.

Diretrizes:

I. Os usuários colaboradores e partes externas devem estar conscientes dos requisitos de segurança da informação e comunicações dos ativos da organização, associados à informação e aos recursos de processamento da informação.
II. Os usuários colaboradores ou externos são responsáveis pelo uso de qualquer recurso de tecnologia da informação que estejam sob sua posse ou uso.
III. O uso de equipamentos e recursos computacionais, incluindo os pessoais, conectados às redes da AMPREV é controlado, estando sujeito a inspeções eventuais.
IV. Todas as mensagens produzidas e transmitidas utilizando recursos de comunicação da organização são de propriedade da Amapá Previdência.
V. A utilização dos recursos corporativos como e-mail, comunicação unificada, Intranet e Internet, deve ser orientada para as atividades de interesse da AMPREV.
VI. As redes sociais acessadas por meio da rede corporativa devem ter como finalidade principal a prestação de serviços públicos ao cidadão.
VII. As informações sensíveis, em papel ou em mídia de armazenamento eletrônica, devem ser guardadas em local seguro.
VIII. Em casos de ausência do usuário responsável, os equipamentos utilizados pelo mesmo, devem ser mantidos desligados ou protegidos com mecanismo de travamento de tela e teclados controlados por senha, *token* ou mecanismo de autenticação semelhante.
IX. Documentos contendo informações sensíveis e críticas devem ser imediatamente, removidos de impressoras após a impressão.
X. Papéis, livros, lembretes, anotações ou qualquer informação confidencial não devem ser deixados na mesa.
XI. Informações confidenciais ou pessoais devem ser mantidas em local apropriado, preferencialmente trancadas.
XII. É proibido que funcionários, fornecedores e partes externas comprometam a Amapá Previdência, através de, por exemplo, difamação, assédio, falsa identidade, retransmissão de “correntes”, compras não autorizadas, entre outros.
XIII. Evitar retransmissão automática de mensagens eletrônicas corporativas de e-mail para endereços externos.
XIV. Os usuários colaboradores devem se atentar para não manterem conversas confidenciais em locais públicos, escritórios abertos, canais de comunicação inseguros e locais de reunião.
XV. É proibido divulgar ou compartilhar indevidamente, informações sigilosas através de dispositivos móveis.
XVI. Os dispositivos móveis devem ser utilizados de forma adequada, prevenindo ações que possam danificar, sobrecarregar ou inutilizar os recursos tecnológicos da Amapá Previdência.
XVII. Os usuários são pessoalmente responsáveis por todas as atividades realizadas por seus dispositivos móveis ao utilizar às redes e recursos da Amapá Previdência.
XVIII. Os usuários somente podem realizar acesso remoto aos recursos de tecnologia da AMPREV, quando previamente autorizados e suas atividades estejam relacionadas com a função exercida.

XIX. Os equipamentos dos usuários que utilizam acesso remoto aos recursos da AMPREV devem estar devidamente atualizados e protegidos por firewall e soluções de antivírus.

XX. Todo acesso remoto configurado deve prover alto nível de segurança, com autenticação e criptografia forte.

XXI. Os usuários são expressamente proibidos de instalar qualquer programa nos computadores da Amapá Previdência, incluindo atualizações que possam comprometer o correto funcionamento dos sistemas organizacionais. As solicitações referentes à instalação de *software* devem ser dirigidas à Divisão de Informática, por meio dos gestores dos setores requisitantes.

6.6 Proteção contra *malware*

Objetivos: Garantir que as informações e os recursos de processamento da informação estejam protegidos contra *malware*.

Diretrizes:

I. É expressamente proibida a utilização de *softwares* não autorizados.

II. Controles através de *firewalls* de aplicação devem ser configurados, para prevenir e detectar o uso de *software* não autorizado.

III. Restringir e registrar a tentativa de acesso a *websites* maliciosos ou suspeitos, por parte dos usuários.

IV. Os usuários devem adotar precauções de examinar com ferramenta antivírus, arquivos e *softwares* importados de redes ou mídias externas.

V. Deve-se instalar e atualizar periodicamente *software* de detecção e remoção de *malware* para a varredura de computadores e mídias magnéticas.

VI. Isolar, ao máximo possível, ambientes críticos que possam ser contaminados por *malwares* para evitar impactos catastróficos às atividades do negócio.

VII. Configurar varreduras automáticas e completas, para serem realizadas regularmente por soluções de antivírus.

6.7 Segurança nas comunicações

Objetivos: Garantir a proteção das informações e dos recursos de processamento que as suportam dentro dos meios de comunicação disponibilizados pela organização.

Diretrizes:

I. Meios devem ser adotados para estabelecer a proteção da confidencialidade e integridade dos dados que trafegam sobre as redes públicas ou sobre as redes sem fio, bem como dos sistemas e aplicações a elas conectados.

II. Aplicar mecanismos apropriados de registro e monitoração para habilitar a gravação e detecção de ações que possam afetar, ou ser relevantes para segurança da informação.
III. Todos os sistemas organizacionais utilizados através de redes devem requerer autenticação e criptografia apropriada.
IV. Utilizar ferramentas e soluções de segurança como *firewalls* e sistemas de detecção e prevenção de intrusão.
V. Segregar redes tanto cabeadas quanto sem fio, estabelecendo políticas de acesso apropriadas tanto quando o acesso for direcionado para Internet quanto entre as próprias redes segregadas.
VI. Mensagens de correio eletrônico (e-mail) são inseguras e não garantem sigilo e entrega. Informações confidenciais e críticas não devem utilizar este meio de comunicação.

6.8 Relacionamento na cadeia de suprimento

Objetivos: Prover a proteção dos ativos da organização que são acessados pelos fornecedores, assim como assegurar que os serviços prestados estão sendo entregues em consonância com os acordos contratuais estabelecidos.

Diretrizes:

I. Definir tipos de acesso à informação a diferentes tipos de fornecedores com regras de segurança bem definidas e monitoramento das atividades desempenhadas pelos fornecedores.
II. Aplicar treinamento de conscientização para os usuários da organização envolvidos com aquisição, relativo aos procedimentos, processos e políticas aplicáveis.
III. Estabelecer condições sob as quais os controles e requisitos de segurança da informação serão documentados em um acordo, assinado por ambas as partes.
IV. Os acordos com os fornecedores devem ser documentados para assegurar que não existam desentendimentos entre a AMPREV e o fornecedor, com relação à obrigação de ambas as partes com o cumprimento dos requisitos de segurança da informação e comunicações.
V. É importante, que no acordo com o fornecedor, conste uma lista explícita do pessoal do fornecedor autorizado a acessar ou receber as informações da Amapá Previdência ou as condições e procedimentos para autorização e remoção de acesso ou recebimento de tais informações pelo pessoal do fornecedor.
VI. Obter garantia de que os produtos de tecnologia da informação e comunicação entregues pelos fornecedores estão funcionando conforme esperado, sem quaisquer características não desejadas ou não esperadas.
VII. Os serviços executados pelos fornecedores serão monitorados, analisados criticamente e auditados a intervalos regulares.
VIII. A monitoração e análise crítica dos serviços executados pelos fornecedores devem garantir que os termos e condições dos acordos de segurança da informação sejam cumpridos e que os

incidentes e problemas de segurança da informação e comunicações sejam gerenciados de forma apropriada.

IX. Os fornecedores devem garantir que a capacidade de serviço seja suficiente, para assegurar que os níveis de continuidade do serviço acordados sejam mantidos, no caso de um desastre ou falha dos serviços principais.

6.9 Tratamento de incidentes de segurança da informação

Objetivos: Gerir os incidentes de segurança da informação, incluindo a comunicação sobre vulnerabilidades e eventos de segurança da informação.

Diretrizes:

I. É necessário que sejam estabelecidas responsabilidades e procedimentos para tratamento de incidentes, como forma de garantir respostas rápidas e efetivas.
II. Implantar um canal de comunicação de incidentes de segurança da informação, de modo que todos os funcionários e colaboradores possam notificar sobre os eventos detectados.
III. Implantar ferramentas de monitoramento de sistemas, que sejam versáteis e capazes de emitir alertas de vulnerabilidades e indisponibilidade dos serviços e sistemas organizacionais da Amapá Previdência.
IV. Todos os funcionários e colaboradores são responsáveis por notificar qualquer evento de segurança da informação, assim que esses eventos forem detectados, ou o mais breve possível.
V. Os conhecimentos obtidos de análise e resolução de incidentes anteriores devem ser utilizados para reduzir as possibilidades de ocorrência ou impacto de incidentes futuros.
VI. Planejar e implantar planos de contingência, como resposta aos incidentes, para manter a continuidade do negócio em um nível aceitável.

6.10 Conformidade

Objetivos: Impedir a violação de quaisquer normas legais, regulamentares ou contratuais relacionadas à segurança da informação.

Diretrizes:

I. É necessário que os gestores identifiquem toda a legislação aplicável à Amapá Previdência, para atender aos requisitos relativos à natureza do negócio desempenhado pelo órgão.
II. Adquirir apenas *softwares* de fontes conhecidas e bem reputadas, para garantir que o direito autoral não esteja sendo violado.
III. Implementar controles que garantam que o número máximo de usuários por licença de *software*, não esteja sendo excedido.

IV. Os sistemas de informação da AMPREV devem ser analisados a intervalos regulares, para verificar a conformidade com as normas e políticas de segurança da informação do órgão.

V. Todas as atividades, sistemas e serviços desenvolvidos e prestados pela Amapá Previdência devem estar em consonância com as leis, normas e regulamentações jurídicas municipais, estaduais e federais vigentes.

7 PENALIDADES

O colaborador que não respeitar ou infringir qualquer diretriz elencada por esta Política estará sujeito a penalidades que vão desde o bloqueio de todos os seus acessos aos sistemas e recursos da AMPREV, até àquelas previstas em lei e nos regulamentos internos da Amapá Previdência.

8 COMPETÊNCIAS E RESPONSABILIDADES

A Política de Segurança da Informação e Comunicações da Amapá Previdência deve ser transmitida a todos os colaboradores da organização, através de um processo de conscientização constante. Todas as ações de divulgação e conscientização dos colaboradores deverão ser coordenadas pela alta gestão da Amapá Previdência, apoiada pela Divisão de Informática e demais setores competentes.

9 VIGÊNCIA E ATUALIZAÇÕES

Esta Política entra em vigor a partir da data de sua aprovação e publicação pela alta Direção da Amapá Previdência.

A Política de Segurança da Informação e Comunicações da Amapá Previdência deverá ser revisada e atualizada, a intervalos regulares de pelo menos um ano, ou quando eventos relevantes ocorrerem que justifiquem tal atualização.

10 REFERÊNCIAS

As referências utilizadas para concepção desta Política foram:

- ABNT NBR ISO/IEC 27002:2013 Tecnologia da informação – Técnicas de segurança – Código de prática para controles de segurança da informação.
- Instrução Normativa GSI/PR Nº 1 – 13/06/2008.
- Normas Complementares da IN GSI/PR Nº 1, DSIC/GSIPR Nº 1 e Nº 5.
- Política de Segurança da Informação e Comunicações da DATAPREV.
- Resolução Nº 1.168/2017-GP do Tribunal de Justiça do Estado do Amapá – TJAP
- Política de Segurança da Informação (13/08/2013) do Instituto Federal de Educação, Ciência e Tecnologia Farroupilha.
- Política de Segurança da Informação – PSI, SEBRAE PREVIDÊNCIA. (AGOSTO/2016)
- PORTARIA Nº 486/2017 – Política de Segurança da Informação do Instituto de Previdência Social dos Servidores Públicos Municipais de Santos.
- PORTARIA Nº 090/2017 – GP/MANAUS PREVIDÊNCIA