RESOLUÇÃO n.º 08/2024, DE 22 DE FEVEREIRO DE 2024.

DISPÕE SOBRE A APROVAÇÃO DA POLÍTICA DE SEGURANÇA DAS INFORMAÇÕES DO INSTITUTO DE PREVIDÊNCIA SOCIAL DOS SERVIDORES PÚBLICOS DO MUNICÍPIO DE TAIÓ/SC - TAIOPREV.

MÁRCIO FARIAS, Presidente do Conselho de Administração do Instituto de Previdência Social dos Servidores Públicos do Município de Taió/SC - TAIOPREV, no uso de suas atribuições conferidas por Lei, disposta no Art. 157 da Lei Ordinária nº 3.625, de 19 de dezembro de 2012 e,

Considerando a necessidade de adequação ao programa de Certificação Institucional e Modernização da Gestão dos Regimes Próprios de Previdência Social da União, dos Estados, do Distrito Federal e dos Municípios (Portaria MPS nº 185/2015 e suas alterações posteriores) – Pró-Gestão RPPS;

Considerando a aprovação constante em Ata da reunião do conselho de administração realizada no dia 22 de fevereiro de 2024:

RESOLVE:

Art. 1º. O Conselho de Administração do Instituto de Previdência Social dos Servidores Públicos do Município de Taió/SC - TAIOPREV, no uso de suas atribuições conferidas pela Lei Municipal nº 3.625, de 19 de dezembro de 2012, aprovou a Política de Segurança das Informações, na segunda reunião ordinária realizada em 22 de fevereiro de 2024, nos termos do texto anexo.

Art. 2º. Esta resolução entrará em vigor na data de sua publicação.

Taió, 22 de fevereiro de 2024.

MÁRCIO FARIAS
Presidente do conselho de Administração do TAIÓPREV

ESTE ATO FOI PUBLICADO NO:
Dom 5684067
Em: 04/03/2024
Assinatura

ANEXO I

POLÍTICA DE SEGURANÇA DE INFORMAÇÕES

CAPÍTULO I
DOS OBJETIVOS E FINALIDADES

Art. 1º Esta política de segurança das informações – (PSI – TAIÓPREV), tem como objetivo reduzir os riscos relacionados à utilização daInternet e de dispositivos eletrônicos e evitar prejuízos financeiros, bem como impactos negativos a imagem do TAIÓPREV, sendo elaborada visando orientar os servidores, conselheiros e prestadores de serviço, para uma utilização mais segura dos recursos de tecnologia da informação disponibilizados assegurando a continuidade dos serviços prestados com a redução dos riscos que possam interferir no alcance dos objetivos da Autarquia.

Art. 2º A PSI - TAIÓPREV tem por finalidade:

I - Estabelecer as estratégias e as definições de responsabilidades e competências para a implantação da gestão de segurança da informação;

II - Implementar a política de proteção das informações contra acesso não autorizado, manutenção da confidencialidade, da integridade e disponibilidade das informações utilizadas nas relações com o TAIÓPREV;

III - Fomentar o gerenciamento de riscos, prevenir e minimizar os impactos dos incidentes de segurança para que seja preservado o patrimônio físico e digital desta entidade;

VI - Definir e estimular o papel e as responsabilidades de cada um dos envolvidos que recebam, guardem, gerenciem, tenham acesso ou administrem informações públicas ou privadas relativas a esta Autarquia.

Art. 3º. Esta Política se aplica a todos os agentes públicos, colaboradores e visitantes que tenham acesso às instalações ou ambientes computacionais e a ativos de informação pertencentes ou sob custódia do TAIÓPREV, bem como a todos os sistemas de informação, processos e procedimentos corporativos, relacionamentos firmados entre a Autarquia e outros órgãos ou entidades, sejam elas públicas ou privadas.

Art. 4º. Todas as medidas cabíveis devem ser tomadas para preservar a integridade e a confidencialidade da informação, a fim de protegê-las de alteração, destruição ou divulgação não autorizada.

CAPÍTULO II
DOS CONCEITOS

Art. 5º. Para fins da PSI - TAIÓPREV, considera-se:

I - Acesso: ato de ingressar, transitar, conhecer ou consultar a informação, bem como a acessibilidade de usar os ativos de informação de um órgão ou entidade;

II - Alta Administração: Diretor- Presidente, Diretor (a) Administrativo Financeiro e Órgãos Colegiados (Conselho Fiscal e Conselho Administrativo);

III - Ameaça: fatores externos ou causa potencial de um incidente de segurança da informação indesejado, que pode resultar em dano para um sistema ou organização;

IV - Arquivo: local físico no qual fica armazenada a documentação do TAIÓPREV em fase intermediária;

V - 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;

VI - Autenticidade: garantia de que a informação é proveniente da fonte anunciada e que não foi alvo de mutações ao longo de um processo;

VII - Autoridade classificadora: pessoa responsável por classificar, desclassificar, reclassificar e reavaliar informação classificada em qualquer grau de sigilo, de ofício ou sob demanda;

VIII - Autoridade hierarquicamente superior: pessoa responsável, juntamente com a autoridade classificadora, por reavaliar informação classificada em qualquer grau de sigilo, de ofício ou sob demanda;

IX - Código de Classificação de Documentos do TAIÓPREV: é o esquema de distribuição de documentos em classes, de acordo com métodos de arquivamento específicos, elaborado a partir do estudo das estruturas e funções de uma instituição e da análise do arquivo por ela produzido;

X - Comitê Gestor de Segurança da Informação: grupo multidisciplinar composto por membros do TAIÓPREV, com o objetivo de avaliar a estratégia, as diretrizes, bem como a operacionalização do cumprimento da política de segurança da informação e do tratamento de dados pessoais estabelecidos pela Autarquia;

XI - Confidencialidade: garantia de que a informação seja acessível somente pelas pessoas autorizadas;

XII - Dado Pessoal: informação relacionada a pessoa natural identificada ou identificável, conforme Lei Federal n. º 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados - LGPD), Art. 5º, Inciso I;

XIII - Dado Pessoal Sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico o político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural, conforme Lei Federal n. º 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados - LGPD), Art. 5º, Inciso II;

XIV - Dado Anonimizado: dado relativo a titular que não possa ser identificado considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento, conforme Lei Federal n. º 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados - LGPD), Art.5º, Inciso III;

XV - Disponibilidade: garantia de que a informação esteja disponível para as pessoas autorizadas sempre que se fizer necessária;

XVI - Gestão documental: conjunto de procedimentos e operações técnicas referentes à produção, tramitação, uso, avaliação e arquivamento dos documentos em fase corrente e intermediária, visando a sua eliminação ou o seu recolhimento para guarda permanente;

XVII - Informação: conjunto de dados organizados, processados ou não, que apresentam um conteúdo de valor e podem ser utilizados para produzir ou repassar conhecimento, contidos em qualquer meio, suporte ou formato;

XVIII - Informação Confidencial: informação cuja exposição fora do ambiente destre Instituto ou da Prefeitura de Taió pode acarretar perdas de capital social, humano, político, financeiro, dentre outros, e que, portanto, não deve ser publicizada, demandando a necessidade de implementação de controles de acesso e de integridade;

XIX - Informação Interna: informação cujo conhecimento por pessoas de fora do ambiente deste Instituto ou da Prefeitura de Taió não é desejável, entretanto, se expostas, não acarretariam perdas de capital social, humano, político, financeiro, dentre outros, demandando apenas a implementação de mecanismos de proteção a sua integridade;

XX - Informação Pública: informação cujo conhecimento pode ser publicizado, embora, seja recomendado o estabelecimento de mecanismos para a sistematização de seu acesso;

XXI - Informação Restrita: informação que pode causar graves danos ao Instituto ou à Prefeitura de Taió se tornada de conhecimento tanto do público interno como do público externo ao ente municipal. Por sua natureza, o seu acesso demanda alto grau de proteção, com prévia liberação formal de autoridade competente e diretamente implicada, fazendo-se necessário a implementação de sólidos mecanismos de controle de acesso e de integridade.

XXII - Integridade: garantia que a informação esteja completa e íntegra e que não tenha sido modificada ou destruída de maneira não autorizada ou acidental durante o seu ciclo de vida;

XXIII - Legalidade: garantia de que as ações sejam realizadas em conformidade com os preceitos legais vigentes e que seus produtos sejam válidos juridicamente;

XXIV - Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador, conforme disposição da Lei Federal n. º 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados - LGPD), em especial o Art. 5º, inciso VII;

XXV - Princípio do menor privilégio: limitação dos direitos de acesso dos usuários apenas ao que é estritamente necessário para a realização dos seus trabalhos;

XXVI - Recursos de tecnologia da informação: microcomputadores, notebooks, tablets, servidores, celulares e smartphones, periféricos associados aos computadores (câmeras, mouse, teclado, caixa de som, microfones, etc.) e demais acessórios (scanners, impressoras a laser, jato de tinta, matriciais e térmicas, etc.), redes de comunicação de dados e voz e os equipamentos relacionados, câmeras de monitoramento e os equipamentos de controle de acesso, equipamentos de projeção e painel de chamada, os softwares desenvolvidos e disponibilizados pelo TAIÓPREV, dados armazenados em equipamentos, dispositivos e periféricos e demais equipamentos relacionados à tecnologia da informação que venham a integrar o patrimônio do TAIÓPREV;

XXVII - Segurança da informação: conjunto de medidas eficazes para resguardar os recursos tecnológicos e viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações, garantindo que somente sejam acessadas por aqueles que devem conhecê-las, evitando seu uso indevido, inadequado, ilegal ou em desconformidade com esta Política;

XXVIII - Tabela de temporalidade: determina prazos e condições de guarda tendo em vista a transferência, recolhimento, descarte ou eliminação de documentos;

XXIX - Tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração, conforme descrito na Lei Federal n. º 13.709, de 14 de agosto de 2018(Lei Geral de Proteção de Dados - LGPD), em especial Art. 5º, Inciso X;

XXX - Usuário externo: pessoa física ou jurídica que tenha acesso concedido a informações produzidas ou recebidas pelo TAIÓPREV e que não seja caracterizada como usuário interno;

XXXI - Usuário interno: empregado público, servidor público, contratado, estagiário ou conveniado da Administração Municipal que, no exercício de suas funções, tenha acesso a informações produzidas ou recebidas pelo TAIÓPREV.

CAPÍTULO III
DAS REGRAS GERAIS E DAS VEDAÇÕES

Art. 6º As informações, em formato físico ou lógico, e os recursos de tecnologia da informação utilizados pelos usuários são de exclusiva propriedade do TAIÓPREV ou da Prefeitura Municipal de Taió, não podendo ser interpretados como de uso pessoal.

Art. 7º Todos os usuários internos e externos devem ter ciência de que o uso das informações e dos sistemas de informação do TAIÓPREV podem ser monitorados e que os registros assim obtidos poderão ser utilizados para detecção de violações desta Política e das Normas de

Segurança da Informação, podendo servir de evidência para a aplicação de medidas disciplinares cabíveis, bem como para processos administrativos ou judiciais.

Parágrafo único. Os usuários internos e os externos estão sujeitos a esta Política e às normas de segurança da informação nela estabelecidas.

Art. 8º Todo processo durante seu ciclo de vida deve garantir, sempre que possível, a segregação de funções, por meio da participação de mais de uma pessoa ou equipe.

Parágrafo único. Todas as informações devem estar adequadamente protegidas em observância às diretrizes de segurança da informação do TAIÓPREV em todo o seu ciclo de vida, que compreende: coleta, retenção, processamento, compartilhamento e eliminação.

Art. 9º O acesso às informações e o uso dos sistemas e aplicativos deverão ser feitos mediante identificação do usuário único, pessoal e intransferível, com utilização de senha de acesso.

§ 1º As informações devem ser utilizadas de forma transparente e apenas para finalidade para a qual foi coletada.

§ 2º Cabe ao usuário a responsabilidade quanto ao sigilo das suas senhas de acesso aos recursos de tecnologia da informação e comunicação do TAIÓPREV.

§ 3º Os sistemas de informação em uso no TAIÓPREV deverão, obrigatoriamente, disponibilizar a função de histórico de logs, a fim de recuperar histórico de ações de cada usuário nos sistemas sempre que necessário para fins de auditoria.

Art. 10. É vedado a qualquer usuário do TAIÓPREV o uso dos recursos de tecnologia da informação para fins pessoais, próprios ou de terceiros, veiculação de opiniões político partidárias ou religiosas, bem como para praticar ações que, de qualquer modo, possam constranger, assediar, ofender, caluniar, ameaçar, violar direito autoral ou causar prejuízos a qualquer pessoa física ou jurídica, assim como aquelas que atentem contra a moral e a ética ou que prejudiquem o cidadão ou a imagem da Autarquia ou do Município de Taió , comprometendo a integridade, a confidencialidade, a confiabilidade, a autenticidade ou a disponibilidade das informações.

CAPÍTULO IV
DA GESTÃO DE ACESSOS E DAS IDENTIDADES

Art. 11. O acesso às informações e aos ambientes tecnológicos do TAIÓPREV deve ser controlado de acordo com a sua classificação, de forma a garantir acesso apenas às pessoas autorizadas, pela alta administração.

Parágrafo único. Os acessos dos usuários internos devem ser solicitados por meio da chefia imediata e dos externos devem ser requeridas à Diretoria Executiva do TAIÓPREV, devendo

ser aprovados os acessos somente às informações necessárias ao desempenho de suas atividades.

Art. 12. O uso dos recursos de tecnologia da informação do TAIÓPREV deve ser passível de monitoramento e auditoria, de forma a serem implementados e mantidos mecanismos que permitam sua rastreabilidade, acompanhamento, controle e verificação de histórico de acessos individuais aos sistemas corporativos e à rede interna do Instituto.

Parágrafo único. Caso sejam identificadas mudanças ou fragilidades quanto ao uso de ativos de informações durante o monitoramento ou a auditoria, elas deverão ser reportadas imediatamente a Diretoria executiva TAIÓPREV.

Art. 13. A sistematização da gestão de acessos tem por objetivo garantir que o acesso à informação e aos recursos tecnológicos que a armazenam sejam franqueado exclusivamente a pessoas autorizadas, com base nos requisitos de negócio e de segurança da informação, sendo passível de monitoramento com vistas a garantir a rastreabilidade e a auditoria das ações realizadas.

Art. 14. Os sistemas que tratam informações restritas deverão ter mais de um fator de autenticação.

Seção I
Do Controle de Acessos

Art. 15. O controle de acesso, credenciais e perfis dos usuários deverá observar as seguintes operações, dentre outras que se façam necessárias:

I - Por ocasião do ingresso dos usuários, mediante:
a) criação de perfis de usuários com nível de autorização adequado às atividades empenhadas;
b) concessão de credenciais de acesso;
c) acesso aos ativos e sistemas necessários à execução de suas atividades proporcionando a rastreabilidade das ações realizadas;
d) entrega de compromisso assinado de não divulgação de informações confidenciais ou restritas a que venha a ter acesso, ainda que após o seu desligamento ou movimentação.

II - Por ocasião do desligamento ou movimentação dos usuários, mediante:
a) arquivamento de histórico de logs dos usuários nos sistemas de que faziam uso;
b) desabilitação dos respectivos perfis de usuários;
c) revogação das credenciais de acesso;
d) devolução de todos os ativos de informação e recursos de tecnologia da informação do TAIÓPREV que estejam em sua posse.

Parágrafo único. Será considerado o princípio do menor privilégio na configuração das credenciais ou concessão de acesso aos ativos de informação.

Seção II
Da Segurança Física

Art. 16. A segurança física se baseia no acesso físico das pessoas aos ambientes que tenham equipamentos de tecnologia da informação, garantindo a proteção de equipamentos de acessos não autorizados, limitando assim a circulação apenas de pessoas treinadas, capacitadas e autorizadas para manuseio desses equipamentos com propósito principal prevenir os danos e possíveis interferências nos recursos de processamento das informações devido ao acesso físico não autorizado.

Art. 17. Será assegurado o controle de acesso e a salvaguarda das instalações e dos ativos de informação em que são elaborados, tratados, custodiados, manuseados ou guardados dados e informações críticas ou sensíveis, independentemente do meio em que estão armazenados.

Art. 18. Toda e qualquer pessoa que necessitar ingressar no TAIÓPREV, deverá ser devidamente identificada no momento de sua recepção.

§ 1° Acesso de terceiros que adentrar nas dependências internas do TAIÓPREV deverá ser acompanhada durante toda sua permanência, por um servidor do Instituto.

§ 2° É vetada a entrada de qualquer pessoa não autorizada nas dependências internas do TAIÓPREV.

§ 3° O acesso às áreas em que são processadas ou armazenadas informações sensíveis é restrito apenas ao pessoal técnico autorizado e a equipe técnica do TAIÓPREV.

Art. 19. O controle e monitoramento do acesso físico, bem como a proteção contra ameaças externas e do meio ambiente nas dependências do prédio até a porta do TAIÓPREV é de total responsabilidade da administração predial onde a Instituição está instalada.

Art. 20. As instalações de armazenagem de dados da tecnologia da informação devem ser protegidas de forma a evitar acesso não autorizado.

Seção III
Da Política de Senhas

Art. 21. A senha é a forma mais convencional de identificação e acesso do usuário, é um recurso pessoal e intransferível que protege a identidade do servidor, evitando que uma pessoa, se faça passar por outra. O uso de dispositivos e/ou senhas de identificação de outra pessoa constitui crime tipificado no Código Penal Brasileiro (art. 307 - Falsa Identidade). Com o objetivo de orientar a criação de senhas seguras, ficam estabelecidas as seguintes regras:

I. A senha é de total responsabilidade do servidor, sendo proibida a sua divulgação ou empréstimo, devendo a mesma, ser imediatamente alterada no caso de suspeita de uso indevido;
II. A senha do e-mail será fornecida pelo setor de T.I no ato da posse do servidor;
III. As credenciais não poderão ser fornecidas por telefone, comunicador instantâneo ou outra forma que não assegure a identidade do servidor;

IV. É obrigatório aos servidores, zelarem pela confidencialidade de sua senha de acesso, podendo ser responsabilizados pelas operações realizadas com a utilização de suas credenciais;

V. A equipe técnica do TAIÓPREV deverá possuir contas e senhas individualizadas com privilégios administrativos e somente deverão utilizar essas contas para o desempenho de suas atividades;

VI. As senhas de acesso à rede de computadores e aos sistemas informatizados devem ser alteradas conforme necessidade;

VII. Fica proibido o compartilhamento de "login" para funções de administração de sistemas;

VIII. As senhas sob hipótese alguma devem ser anotadas e deixadas próximo a computador (debaixo do teclado, colada no monitor, etc.);

IX. As senhas deverão seguir os seguintes pré-requisitos:
e) Tamanho mínimo de 08 (oito) caracteres;
f) Existência de caracteres pertencentes a, pelo menos, 03 (três) dos seguintes grupos: letras maiúsculas, letras minúsculas, números e caracteres especiais.

Seção IV
Acesso À Rede

Art. 22. Todos os servidores, membros de Conselhos e colaboradores estão autorizados e poderão fazer uso dos recursos da rede corporativa TAIÓPREV, tais como:
I - Correio eletrônico (e-mail)
II - Internet, intranet;
III - Compartilhamento e armazenamento de arquivos;
IV - Estações de trabalho;
V - Softwares e sistemas de informação;
VI - Serviços de impressão.

Art. 23. Os servidores, membros de Conselho e colaboradores terão acesso unicamente e exclusivamente àqueles recursos da rede corporativa TAIÓPREV que lhe forem indispensáveis à realização de suas atividades.

Art. 24. Sob nenhuma hipótese os servidores que utilizam os recursos de rede disponibilizados pelo TAIÓPREV poderão utilizá-los para fazer o download ou distribuição de software pirateados, atividade considerada delituosa de acordo com a legislação nacional vigente.

Seção V
Estações De Trabalho

Art. 25. Constituem estações de trabalho os computadores e notebooks registrados como patrimônio do TAIÓPREV, e utilizados pelos servidores no desempenho de suas atividades funcionais. Assim recomendamos algumas medidas de segurança que devem ser adotadas quanto à utilização das estações de trabalho:

I. Não sejam instalados softwares sem a autorização;

II. Só sejam utilizados softwares devidamente licenciados;

III. A utilização de software não licenciado ou considerado "pirata" constitui infração prevista na Lei Federal n. º 9.609/1998;

IV. Fica proibido remover ou modificar qualquer software ou hardware sem a autorização da área de tecnologia do TAIÓPREV, uma vez que tal atitude pode comprometer a segurança e o desempenho da estação de trabalho;

V. Ao se ausentar da estação de trabalho, efetue o bloqueio ou "logoff" da mesma, evitando assim os acessos indevidos de outra pessoa através do seu usuário (login);

VI. A liberação do dispositivo móvel (notebook) será permitida após os solicitantes assinarem o acordo de conhecimento das suas responsabilidades (quanto a proteção física, atualização do software, entre outros), renunciando direitos autorais dos dados, que permita a exclusão remota dos dados pelo TAIÓPREV;

VII. Em caso de furto/roubo ou perda do dispositivo móvel, o servidor deverá comunicar imediatamente as autoridades policiais registrando, assim um boletim de ocorrência e deverá ainda comunicar a chefia imediata;

VIII. Utilização da estação somente para fins profissionais.

Seção VI
Equipamentos Particulares e Dispositivos Móveis

Art. 26. Ficam estabelecidas as seguintes regras para o uso de equipamentos particulares e de dispositivos moveis no âmbito do TAIÓPREV:

I. A liberação para utilização de notebooks e para acesso à internet do TAIÓPREV se dará mediante solicitação justificada e assinatura do termo de compromisso, vide Anexo I

II. O uso de notebooks particulares para fins de acesso à rede de Internet do TAIÓPREV, será realizado mediante a verificação se tal equipamento possui proteção apropriada para uso autorizado;

III. Sob hipótese alguma poderão ser executados nos notebooks, software de característica maliciosa, que visam comprometer o funcionamento da rede;

IV. É de responsabilidade do proprietário usar somente software legalizados em seu notebook;

V. É proibido o armazenamento de informações de propriedade do TAIÓPREV;

VI. Todos os arquivos que pertençam ao TAIÓPREV não poderão ser armazenados no disco rígido do notebook e/ou em dispositivos de armazenamento móvel, como exemplo: pendrive e/ou armazenamento em nuvem pessoal;

VII. É proibida a inclusão de smartphones na rede corporativa TAIÓPREV, salvo mediante aprovação da Diretoria Executiva.

Seção VII
E-Mail Corporativo

Art. 27. O serviço de correio eletrônico (e-mail corporativo) é permitido somente para as atividades profissionais de seus usuários, não sendo permitido enviar ou arquivar mensagens que não estejam relacionadas às atividades deste TAIÓPREV, e que contenham:

I. Assuntos que provoquem assédio, perturbação a outras pessoas ou que prejudiquem a imagem do TAIÓPREV;

II. Temas difamatórios, discriminatórios, caluniosos, degradantes, ofensivos, violentos, ameaçadores, materiais obscenos, materiais pornográficos, ilegais ou antiéticos;

III. Fotos, imagens, sons ou vídeos que não tenham relação com as atividades profissionais do TAIÓPREV;

IV. Compartilhar arquivos com códigos executáveis (.exe, .cmd, .pif, .js, .hta, .src, .cpl, .reg, .dll, .inf) ou qualquer outra extensão que possa apresentar risco a segurança da informação do TAIÓPREV.

Seção VIII
Gestão De Mudanças

Art. 28. Todas as mudanças devem ser constituídas, no mínimo, pelas fases de identificação, registro, planejamento, teste preliminar, aprovação, implementação e verificação de potenciais impactos das mesmas por tanto:

I. Toda e qualquer proposta de mudança deve ser aprovada formalmente pela alta gestão juntamente com a equipe técnica competente;

II. Toda mudança realizada no TAIÓPREV deverá ser devidamente comunicada à todas as partes interessadas;
III. Deverá ser amplamente divulgada, visando a redução de eventuais resistências e dificuldades de implementação das mesmas;

IV. Toda mudança, antes de ser implementada, deve contar com um plano de recuperação emergencial, incluindo procedimentos e responsabilidades para interrupção e recuperação, em caso de insucesso ou na ocorrência de eventos inesperados.

CAPÍTULO V
DA GESTÃO DE RISCOS E INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Art. 29. A gestão de riscos de segurança da informação deve ser realizada de forma sistemática e contínua e englobar todos os ativos de informação do TAIÓPREV, visando a tratar riscos relacionados à disponibilidade, integridade, confidencialidade e autenticidade.

Art. 30. O Comitê de Gestão de Segurança da Informação - CGSI deverá apresentar, em um prazo máximo de 90 (noventa) dias após a publicação em Diário Oficial dos Municípios os seus membros constituintes, plano dispondo sobre os princípios e diretrizes da gestão de riscos à segurança da informação do Instituto.

Art. 31. Em caso de violação desta Política, por ação ou omissão, intencional ou acidental, o Conselho de administração realizará deliberações sobre os incidentes classificados como de alta criticidade.

Parágrafo Único. Após deliberações descritas no *caput*, Conselho de administração recomendará ao Presidente do TAIÓPREV as ações a serem tomadas e este decidirá em conjunto com a Alta Administração sobre sua procedência ou não, sem prejuízo de outras legislações vigentes.

Art. 32. Os contratos entre o TAIÓPREV e as empresas prestadoras de serviços com acesso às informações, aos sistemas e/ou ao ambiente tecnológico da Autarquia devem conter cláusulas que garantam a confidencialidade entre as partes e que assegurem minimamente que os profissionais sob sua responsabilidade cumpram a Política e as Normas de Segurança da Informação estabelecidas a nível municipal e federal.

Art. 33. A manutenção de um ambiente tecnológico seguro é tarefa inerente não só aos administradores e técnicos de informática, bem como a todos os envolvidos na estrutura da Administração Municipal, usuários internos e externos.

CAPÍTULO VI
DO TRATAMENTO E DA CLASSIFICAÇÃO DA INFORMAÇÃO

Art. 34. Toda informação institucional no âmbito do TAIÓPREV deve ser gerida adequadamente com o objetivo de garantir a sua disponibilidade, integridade, autenticidade e, quando aplicável, confidencialidade, independente do meio de armazenamento, processamento ou transmissão utilizado.

Art. 35. A segurança da informação deve ser prevista e realizada em todo o ciclo de vida dos dados, sendo apoiada pelo desenvolvimento de software seguro e sob governança efetivo dos dados.

Art. 36. Todos que tiverem acesso aos ativos de informação do TAIÓPREV devem utilizar preferencialmente as ferramentas de trabalho autorizadas pela Diretoria Executiva, ainda que fora das dependências do TAIÓPREV.

Art. 37. O tratamento das informações pessoais deve considerar o respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais, conforme o disposto na Lei Federal n. º 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados - LGPD), na Lei Federal n. º 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação - LAI).

Parágrafo único. O compartilhamento de dados com outros órgãos ou entidades da Administração Pública deve ser pautado na legislação vigente, considerando as restrições de acesso e sigilo.

CAPÍTULO VII
DOS DEVERES

Seção I
Dos Deveres De Todos Os Usuários

Art. 38. São deveres de todos os usuários:

I - Cumprir fielmente a política, as normas e os procedimentos de segurança da informação do TAIÓPREV;

II - Assinar os Termos de Responsabilidade e Sigilo, bem como os termos de regulamentação do teletrabalho no âmbito do TAIÓPREV, conforme modelos a serem estabelecidos pela Diretoria Executiva do TAIÓPREV.

III - Proteger as informações contra acessos, modificação, destruição ou divulgação não autorizados pelo TAIÓPREV;

IV - Assegurar que os recursos tecnológicos, as informações e sistemas a sua disposição sejam utilizados apenas para as finalidades aprovadas pela Diretoria Executiva do TAIÓPREV;

V - Manter, nas unidades de armazenamento de rede, apenas arquivos que estejam estritamente relacionados às atividades desempenhadas pelo TAIÓPREV, sendo vedada a gravação de arquivos de músicas, fotos, vídeos e outros, que não atendam a tal finalidade;

VI - Tratar os dados dos sistemas informatizados em conformidade com os princípios e práticas dispostos na Lei Federal n.º 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados - LGPD);

VII - Cumprir as leis e as normas que regulamentam a propriedade intelectual;

VIII - Garantir a segurança das informações da Administração Municipal a que tenham acesso;

XI - Utilizar as senhas utilizadas de acordo com as diretrizes fixadas;

XX - Não discutir assuntos confidenciais de trabalho em ambientes públicos ou em áreas expostas, incluindo a emissão de comentários e opiniões em blogs e redes sociais;

XXI - Não compartilhar informações confidenciais de qualquer tipo;

XXII - Colaborar com alertas, sugestões e críticas que possam melhorara segurança da informação;

XXIII - Comunicar imediatamente a Diretoria Executiva e ao seu superior hierárquico, eventos potenciais ou reais de risco, descumprimento ou violação desta política e/ou de suas norma e procedimentos, que tenham presenciado ou de que tenham conhecimento.

Parágrafo único. Após a assinatura dos termos citados no inciso II, o usuário assume formalmente a responsabilidade pelo bom uso dos ativos de informações, compromisso de seguir a PSI - TAIÓPREV e de manter o sigilo, em caráter permanente, sobre todos os ativos de informações, mesmo após o seu desligamento ou término de prestação de serviços.

Seção II
Dos Deveres Da Alta Administração

Art. 39. São deveres da Alta administração do TAIÓPREV:

I - Definir as responsabilidades pela segurança da informação, nas descrições dos cargos e funções, bem como nos termos e condições das contratações que envolvam o manuseio de dados, informações ou conhecimentos do TAIÓPREV;

II - Promover ações para que todos os usuários sejam conscientizados e treinados nos procedimentos de segurança da informação;

III - Assegurar que o controle operacional de uma atividade crítica não seja de atribuição exclusiva de uma única pessoa;

IV - Assegurar que quando houver afastamento, mudança de responsabilidades e de lotação ou, ainda, mudança de atribuições dentro da Autarquia ocorra imediata revisão dos direitos de acesso e uso dos ativos;

V - Assegurar que quando da efetivação do desligamento de usuário, deverão ser extintos todos os direitos de acesso e uso dos ativos a ele atribuídos;

VI - Assegurar que todo o ativo produzido por um usuário desligado seja mantido pelo TAIÓPREV, garantindo o reconhecimento e o esclarecimento da propriedade do acervo para a Instituição;

VII - Monitorar, fiscalizar e auditar a qualquer tempo os procedimentos desempenhados pelo CGSI-TAIÓPREV.

Seção III
Dos Deveres do Setor de Gestão Documental/Arquivo-TAIÓPREV

Art. 40. São deveres do Setor de Gestão Documental/Arquivo – TAIÓPREV:

I - Realizar a gestão documental da Autarquia, bem como orientar os setores internos acerca de procedimentos para acesso à documentação, empréstimos, consultas, arquivamentos, acondicionamentos e classificação da informação dos documentos em meios físicos e digitais;

II - Garantir, por meio da criação e implantação de procedimentos, a integridade, autenticidade, disponibilidade, não repúdio e a confidencialidade dos documentos/processos físicos, digitais e híbridos, produzidos ou recebidos pelo TAIÓPREV, desde a sua entrada até o seu arquivamento e acondicionamento;

III - Estabelecer, Sistema de Classificação e aplicar a Tabela de Temporalidade de Documentos disciplinada em Lei Municipal;

IV - Opinar sobre a informação produzida no âmbito de sua atuação para fins de classificação em qualquer grau de sigilo;

V - Assessorar a autoridade classificadora ou a autoridade hierarquicamente superior quanto à classificação, desclassificação, reclassificação ou reavaliação de informação classificada em qualquer grau de sigilo, conforme Código de Classificação e Tabela de Temporalidade do TAIÓPREV;

VI - Propor o destino final das informações desclassificadas, indicando os documentos para a guarda permanente, conforme Código de Classificação e Tabela de Temporalidade do TAIÓPREV.

Seção IV
Certificado Digital

Art. 41 Certificado digital é um documento eletrônico que identifica pessoas e instituições, provando sua identidade e permitindo acessar serviços informatizados com a garantia de autenticidade, integridade e não-repúdio, assim como assinar digitalmente documentos. O certificado digital destina-se a qualquer pessoa, física ou jurídica, sendo emitido por uma Autoridade Certificadora (AC).

Art. 42 Cada usuário é responsável pela guarda e utilização de seu certificado digital.

Parágrafo único. Não fornecer o certificado digital a terceiros. O certificado digital é um documento pessoal e intransferível.

CAPÍTULO VIII
DISPOSIÇÕES FINAIS

Art. 43. Na ocorrência de violação desta Política ou das normas de segurança da informação, o Diretor Presidente do TAIÓPREV, com o apoio do conselho de administração, poderá adotar, sanções administrativas e/ou legais.

Art. 44. O TAIÓPREV se reserva ao direito de revisar, adicionar, modificar ou atualizar a Política de Segurança da Informação, periodicamente, no máximo a cada 02 (dois) anos, para aprimorar e garantir o perfeito funcionamento das normas e regras nela estabelecidas.

Art. 45. Os casos omissos serão analisados pelo conselho de administração que deverá propor solução ao Presidente do TAIÓPREV.

Art. 46. As normas e procedimentos da PSI -TAIÓPREV não se esgotam neste instrumento, sobretudo em razão da constante evolução tecnológica, não consistindo em rol taxativo, motivo pelo qual é obrigação dos usuários, adotarem todo e qualquer outro procedimento de segurança que esteja ao seu alcance, visando sempre proteger as informações do TAIÓPREV.

Art. 47. A implementação da PSI-TAIÓPREV será feita de forma gradual, de acordo com a disponibilidade técnica, recursos humanos, tecnológicos e financeiros, cujas ações serão priorizadas em virtude de seu grau de relevância, criticidade e impacto e em função dos investimentos envolvidos.

Art. 48. Os casos omissos deverão ser dirimidos pelo Conselho de Administração do TAIÓPREV.

ANEXO II
TERMO DE COMPROMISSO

Nome do solicitante:	
Lotação:	**Cargo:**
Matrícula:	**Telefone:**
Descrição do equipamento a ser liberado (notebook/computador,marca):	
Número de patrimônio:	
Descrição do dispositivo:	
Motivo do uso do dispositivo/sistema:	
Observações:	

Taió, xx de xxxxxxx de 2024

Autorizado por