DECRETO Nº 1.802, de 27 de fevereiro de 2026

Reformula a Política de Segurança da Informação no âmbito do regime próprio de previdência dos servidores públicos municipais de Toledo – Fundo de Aposentadorias e Pensões dos Servidores Públicos Municipais de Toledo – FAPES/TOLEDOPREV.

O PREFEITO DO MUNICÍPIO DE TOLEDO, Estado do Paraná, no uso de suas atribuições legais e em conformidade com o que dispõem a alínea "n" do inciso I do *caput* do artigo 61 da Lei Orgânica do Município e a Lei nº 1.929/2006,

considerando a necessidade de aprimorar a governança e os controles relacionados à segurança da informação no âmbito do Fundo de Aposentadorias e Pensões dos Servidores Públicos Municipais de Toledo – FAPES/TOLEDOPREV;

considerando os requisitos estabelecidos no Manual do Pró-Gestão RPPS, especialmente no item 3.1.5 – Política de Segurança da Informação;

considerando que a reformulação da Política de Segurança da Informação foi aprovada pelo Conselho de Administração do TOLEDOPREV, em reunião realizada no dia 26 de fevereiro de 2026, conforme Ata nº 003/2026 e Resolução nº 009/2026, do mencionado Conselho;

considerando, por fim, a solicitação contida no Ofício nº 018/2026, de 26 de fevereiro de 2026, da Diretora-Executiva do TOLEDOPREV (Processo SEI nº 01.06.007305/2026-10),

D E C R E T A:

Art. 1º - A Política de Segurança da Informação para aplicação no âmbito do regime próprio de previdência dos servidores públicos municipais de Toledo – FAPES/TOLEDOPREV, originariamente instituída pelo Decreto nº 871, de 24 de julho de 2020, fica reformulada por este Decreto.

Art. 2° - Compõem a Política de Segurança da Informação do FAPES/TOLEDOPREV os seguintes Anexos que integram este Decreto:

I - Anexo I – Política de Segurança da Informação – PSI;

II - Anexo II – Política de Classificação da Informação;

III - Anexo III – Plano de Recuperação de Desastres – DRP;

IV - Anexo IV – Manual de Auditoria de Acessos à Informação; e

V - Anexo V – Plano Anual de Capacitação em Segurança da Informação.

Art. 3° - A Política de Segurança da Informação e seus Anexos deverão ser revistos sempre que houverem alterações relevantes no ambiente institucional, tecnológico ou normativo e, no mínimo, a cada 4 (quatro) anos.

Art. 4° - A Política de Segurança da Informação de que trata este Decreto estará disponível, na íntegra, para acesso público, no sítio eletrônico oficial do FAPES/TOLEDOPREV na internet.

Art. 5º - Este Decreto entra em vigor na data de sua publicação.

GABINETE DO PREFEITO DO MUNICÍPIO DE TOLEDO, Estado do Paraná, em 27 de fevereiro de 2026.

MARIO CÉSAR COSTENARO
PREFEITO DO MUNICÍPIO DE TOLEDO

LEANDRO MARCELO LUDVIG
SECRETARIO DE RECURSOS HUMANOS

Publicação: ÓRGÃO OFICIAL ELETRÔNICO DO MUNICÍPIO, nº 4.658 (Extraordinária), de 27/02/2026

ANEXO I

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO – PSI

FUNDO DE APOSENTADORIAS E PENSÕES DOS SERVIDORES PÚBLICOS MUNICIPAIS DE TOLEDO – FAPES/TOLEDOPREV

CAPÍTULO I
DAS DISPOSIÇÕES GERAIS

Art. 1º - Fica instituída, no âmbito do regime próprio de previdência dos servidores públicos municipais de Toledo – FAPES/TOLEDOPREV, doravante denominada TOLEDOPREV, a Política de Segurança da Informação - PSI, destinada às pessoas abrangidas por suas disposições, com a finalidade de estabelecer orientações e procedimentos a serem adotados para o manuseio, controle e proteção das informações sob a guarda da unidade gestora do RPPS, em qualquer meio ou suporte, contra destruição, modificação e/ou divulgação indevidas e acessos não autorizados.

CAPÍTULO II
DO PÚBLICO ABRANGIDO E DAS RESPONSABILIDADES

Art. 2º - Para fins desta Política, consideram-se pessoas abrangidas por suas disposições todos aqueles que, a qualquer título, utilizem, acessem, tratem, produzam, recebam, armazenem, transmitam ou tenham sob sua guarda informações, sistemas, ativos e recursos de tecnologia da informação relacionados às atividades do Fundo de Aposentadorias e Pensões dos Servidores Públicos Municipais de Toledo – FAPES/TOLEDOPREV, incluindo, no que couber:
I - agentes públicos em exercício no TOLEDOPREV;
II - conselheiros, membros de comissões e colaboradores;
III - estagiários e aprendizes;
IV - prestadores de serviços, fornecedores e pessoas físicas ou jurídicas contratadas, bem como seus prepostos; e
V - segurados, beneficiários e dependentes, quando usuários de serviços, canais, sistemas ou informações do TOLEDOPREV.

Parágrafo único - As disposições desta Política aplicam-se, ainda, a quaisquer terceiros que, por força de contrato, convênio, termo de cooperação ou outro instrumento, tenham acesso a informações ou ativos sob responsabilidade do TOLEDOPREV.

CAPÍTULO III
DOS PRINCÍPIOS

Art. 3º - São princípios basilares da Política de Segurança da Informação, no âmbito do TOLEDOPREV:
I - Confidencialidade: proteção e garantia de que determinadas informações só são disponíveis a pessoas autorizadas;
II - Integridade: garantia da exatidão das informações e dos métodos de processamento; e
III - Disponibilidade: garantia de que os usuários autorizados e os interessados tenham acesso às informações.

CAPÍTULO IV
DOS OBJETIVOS

Art. 4º - São objetivos norteadores da Política de Segurança da Informação, no âmbito do TOLEDOPREV:

I - proteger a informação sob a guarda da unidade gestora do Fundo de Aposentadorias e Pensões dos Servidores Públicos Municipais de Toledo, em qualquer meio ou suporte, de vários tipos de ameaças, para garantir a continuidade das atividades no âmbito do TOLEDOPREV, reduzindo os riscos de falhas, danos e prejuízos que possam comprometer os objetivos da instituição;
II - adotar condutas que observem os preceitos legais, de acordo com aspectos de legitimidade, legalidade e justiça;
III - garantir a segurança dos ativos computacionais, instalações prediais e documentos em meio físico, abrangendo, também, o controle de acesso de pessoas às instalações do TOLEDOPREV;
IV - garantir a segurança de toda e qualquer informação contida em meio digital, seja em equipamentos, tráfego de informações pela rede, por correio eletrônico ou armazenado em estações de trabalho dos usuários;
V - promover a educação e conscientização de cada usuário sobre a responsabilidade para com a segurança da informação, por meio de sugestões e ações educativas; e
VI - promover ampla divulgação da Política de Segurança da Informação a todos os servidores efetivos, cedidos, comissionados, temporários, estagiários, conselheiros, segurados, beneficiários, dependentes e pessoas jurídicas ou físicas e fornecedores de serviços contratados pelo TOLEDOPREV.

CAPÍTULO V
DA AUTENTICAÇÃO DE ACESSO AOS SISTEMAS DE GESTÃO

Art. 5º - A autenticação de acesso dos usuários aos sistemas informatizados de gestão do TOLEDOPREV ocorrerá por meio de *login* e senhas individuais e intransferíveis, devendo este conter, no mínimo, 8 (oito) caracteres alfanuméricos (letras e números).

§ 1º - As senhas deverão ser alteradas periodicamente pelos usuários ou sempre que necessário.

§ 2º - Todas as ações executadas por meio do *login* individual serão de inteira responsabilidade do usuário correspondente.

CAPÍTULO VI
DO USO DO CORREIO ELETRÔNICO E DO ACESSO À INTERNET

Art. 6º - A ferramenta de correio eletrônico corporativo constitui meio de comunicação corporativa do TOLEDOPREV, a ser utilizado com nome do órgão/setor/nome, seguido do domínio <@toledo.pr.gov.br>, devendo ser utilizado de acordo com os princípios estabelecidos nesta Política de Segurança da Informação.

§ 1º - É vedado o uso de contas particulares de correio eletrônico para fins institucionais.

§ 2º - Os e-mails encaminhados pelo correio eletrônico corporativo deverão adotar assinatura padrão com as seguintes informações:
I - nome completo do servidor;
II - cargo/Departamento;
III - nome do TOLEDOPREV;
IV - telefone(s); e
V - site do RPPS na Internet.

Art. 7º - Os recursos de internet, correio eletrônico corporativo ou qualquer outro existente ou que venha a ser adotado, deverão ser utilizados em consonância com os interesses do TOLEDOPREV.

Art. 8º - É vedada a falta de moderação no uso do correio eletrônico corporativo, considerando-se abuso a utilização que comprometa o desempenho do servidor em horário de trabalho, a boa imagem e a segurança dos dados do TOLEDOPREV, bem como qualquer outra forma de utilização que fuja à legalidade, à moralidade ou a qualquer outro princípio administrativo.

Art. 9º - É permitida a comunicação instantânea via aplicativos de celular, a exemplo de “Whatsapp”, “Telegram”, etc., e redes sociais, no aparelho celular do TOLEDOPREV, desde que utilizado para fins institucionais, sendo vedado seu uso para fins particulares.

Art. 10 - O acesso recreativo à internet deverá observar, além dos princípios constitucionais da legalidade, moralidade, razoabilidade e demais aplicáveis, as seguintes restrições:
I - proibição do acesso a sites não confiáveis, impróprios, incluídos aqueles com conteúdo sexual ou preconceituoso, jogos, salas de bate-papo, apostas e assemelhados;
II - proibição do uso de ferramentas Peer-to-Peer (P2P), para o compartilhamento de serviços e dados; e
III - proibição do uso e instalação de jogos ou de download de arquivos que comprometam o tráfego da rede (vídeos, imagens, músicas, etc.), para fins particulares.

CAPÍTULO VII
DO USO DA INTERNET PELA REDE WI-FI

Art. 11 - O uso da internet pela rede Wi-Fi (Wireless Fidelity), no âmbito do TOLEDOPREV, é permitido aos servidores efetivos, cedidos, comissionados, temporários, estagiários e conselheiros, desde que para uso profissional, condizente com as tarefas do cargo ou função.

§ 1º - Os usuários deverão conhecer as regras de acesso à referida rede, conforme Política de Uso do Departamento de Tecnologia da Informação da Secretaria de Administração do Município de Toledo, doravante denominado Departamento de Tecnologia da Informação, e estar cientes das penalidades que poderão ocorrer caso haja violação das mesmas.

§ 2º - Para visitantes ou outros usuários não mencionados no caput, será permitido o acesso à internet exclusivamente por meio de dispositivo próprio, em rede específica destinada a visitantes, administrada pelo Departamento de Tecnologia da Informação, sem acesso aos sistemas, redes internas ou dados institucionais do Município.

Art. 12 - A Política de Uso da rede Wi-Fi (Wireless Fidelity), no âmbito do TOLEDOPREV, é constituída pelas seguintes regras:
I - não se fazer passar por outra pessoa ou dissimular sua identidade quando utilizar os recursos computacionais;

II - responsabilizar-se pela sua identidade eletrônica, senha ou outro dispositivo de segurança, negando revelá-la a terceiros;
III - manter seus dispositivos pessoais (notebooks, smartphones, etc.) com softwares e antivírus atualizados;
IV - não usar a rede para trafegar informações confidenciais e/ou sigilosas, salvo quando utilizado algum meio seguro de transmissão (VPN, conexões cifradas, etc.);
V - responder pelo mau uso dos recursos computacionais em qualquer circunstância; e
VI - responder por atos que violem as regras de uso dos recursos computacionais, estando, portanto, sujeito às penalidades definidas na Política de Uso desses recursos.

Art. 13 - Considerar-se-á violação das regras de Política de Uso da rede Wi-Fi (Wireless Fidelity), no âmbito do TOLEDOPREV:
I - infringir qualquer lei ou regulamento local, estadual, nacional ou internacional aplicável;
II - acessar, mostrar, armazenar ou transmitir texto, imagens ou sons que possam ser considerados ofensivos ou abusivos;
III - utilizar os recursos computacionais do TOLEDOPREV para constranger, assediar, ameaçar ou perseguir qualquer pessoa;
IV - efetuar ou tentar efetuar qualquer tipo de acesso não autorizado aos recursos computacionais do TOLEDOPREV;
V - utilizar os recursos computacionais do TOLEDOPREV para invadir, alterar ou destruir recursos computacionais de outras instituições;
VI - interceptar ou tentar interceptar a transmissão de dados através de monitoração;
VII - provocar interferência em serviços de outros usuários ou o seu bloqueio, provocando o congestionamento da rede de dados, inserindo vírus ou tentando a apropriação indevida dos recursos computacionais do TOLEDOPREV;
VIII - utilizar os recursos computacionais do TOLEDOPREV para fins comerciais ou políticos, tais como mala direta, spams ou propaganda política; e
IX - não fazer uso ou divulgar conteúdos impróprios como: pornografia, erotismo, racista, sexista, difamatório, falsos perfis em sites pessoais ou quaisquer outros tipos de ataques dessa categoria.

CAPÍTULO VIII
DAS ESTAÇÕES DE TRABALHO

Art. 14 - Cada servidor no âmbito do TOLEDOPREV deverá utilizar uma estação de trabalho determinada, que deverá ser protegida por senha individual e intransferível, sendo esta composta por, no mínimo, 8 (oito) caracteres alfanuméricos (letras e números).

Art. 15 - O uso das estações do TOLEDOPREV deverá observar, além dos princípios constitucionais da legalidade, moralidade, razoabilidade e demais aplicáveis, as seguintes restrições:
I - proibição do uso de dispositivos móveis de armazenamento sem aplicação de antivírus;
II - proibição do armazenamento, edição ou distribuição de qualquer material de cunho sexual, preconceituoso ou ilegal, incluindo pirataria;
III - proibição do uso indevido de impressoras para fins particulares;

IV - proibição da retirada de equipamentos eletrônicos da sede do TOLEDOPREV, salvo com autorização da Coordenação do TOLEDOPREV;
V - proibição da retirada de arquivos físicos ou digitais da sede do TOLEDOPREV, salvo com autorização da Coordenação do TOLEDOPREV; e
VI - proibição de instalação de softwares ou hardwares não licenciados sem autorização da Coordenação do TOLEDOPREV, ou qualquer outro tipo de pirataria.

Art. 16 - O antivírus deverá estar sempre atualizado, cabendo ao usuário da estação de trabalho informar ao Departamento de Tecnologia da Informação e à Coordenação do TOLEDOPREV quaisquer atitudes suspeitas em sua estação de trabalho ou notificações que venha a receber, incluindo notificações relacionadas ao funcionamento dos programas.

Art. 17 - Todo e qualquer equipamento que componha o parque computacional de uso do TOLEDOPREV só poderá ser retirado mediante o preenchimento de formulário específico, contendo justificativa, assinatura da Coordenação do TOLEDOPREV e do responsável pela retirada.

CAPÍTULO IX
DOS PROCEDIMENTOS BÁSICOS DE SEGURANÇA

Art. 18 - O TOLEDOPREV adotará providências no sentido de garantir:
I - que os equipamentos estejam em bom estado de conservação para atender as demandas do TOLEDOPREV e não comprometam a segurança das informações produzidas;
II - a realização de cópias de segurança (backups) das informações armazenadas nas estações de trabalho e demais ambientes tecnológicos, conforme os procedimentos e diretrizes estabelecidos no Plano de Recuperação de Desastres – DRP (Anexo III), vedada sua disponibilização a terceiros, salvo quando necessária à restauração autorizada ou à execução de procedimentos técnicos pelo Departamento de Tecnologia da Informação ou por empresa previamente autorizada; e
III - a realização de cópias de segurança das informações do correio eletrônico institucional, quando aplicável, observados os procedimentos definidos no Plano de Recuperação de Desastres – DRP (Anexo III) e as normas técnicas vigentes.

Art. 19 - Os usuários de sistemas e serviços de informação do TOLEDOPREV deverão registrar e relatar à Coordenação qualquer observação ou suspeita de fragilidade de segurança das informações armazenadas ou tratadas.

Art. 20 - As evidências dos incidentes de segurança deverão ser coletadas e armazenadas de forma organizada e identificável, sob coordenação da Gestão de Segurança da Informação – GSI, para fins de apuração, adoção de providências e atendimento às auditorias internas e externas.

Art. 21 - O acesso aos documentos armazenados nos arquivos físicos da unidade gestora do TOLEDOPREV somente poderá ocorrer por servidor autorizado, mediante controle formal de retirada e devolução, observadas as normas arquivísticas, a legislação aplicável e as diretrizes da Política de Segurança da Informação.

Parágrafo único - O armazenamento e o acesso aos documentos físicos e digitais deverão observar, especialmente, a Lei de Acesso à Informação, a Lei Geral de Proteção de Dados Pessoais, as normas arquivísticas vigentes e, quando aplicável, as diretrizes técnicas adotadas pelo Município de Toledo.

CAPÍTULO X
DO ACESSO REMOTO

Art. 22 - O acesso remoto de terceiros à rede do TOLEDOPREV será permitido somente para atender aos interesses do TOLEDOPREV, mediante autorização prévia e expressa da Coordenação do TOLEDOPREV e acompanhamento de servidor do Departamento de Tecnologia da Informação.

§ 1º - O acesso remoto deverá ser realizado exclusivamente por meio das ferramentas corporativas oficialmente autorizadas pelo Departamento de Tecnologia da Informação, tais como TeamViewer e VPN institucional, ou outras que venham a substituí-las, desde que garantam requisitos mínimos de segurança da informação, controle de acesso e registro de logs de eventos.

§ 2º - Os terceiros que tenham acesso remoto à rede do TOLEDOPREV deverão observar os seguintes requisitos, sob pena de aplicação das penalidades cabíveis:
I - manter sigilo das informações às quais tiverem acesso, sendo de sua total e exclusiva responsabilidade qualquer operação realizada sob suas credenciais de uso; e
II - comunicar imediatamente à Coordenação qualquer situação que coloque em risco o acesso ao ambiente de rede do TOLEDOPREV.

CAPÍTULO XI
DOS PROCEDIMENTOS DE CONTINGÊNCIAS

Art. 23 - Os procedimentos de contingências em segurança da informação, no âmbito do Fundo de Aposentadorias e Pensões dos Servidores Públicos Municipais de Toledo – FAPES/TOLEDOPREV, correspondem às ações previamente planejadas destinadas a reduzir os impactos de incidentes graves ou desastres que comprometam a disponibilidade, a integridade ou a confidencialidade das informações e dos serviços essenciais.

Art. 24 - Os procedimentos de contingência deverão observar, prioritariamente, as diretrizes, responsabilidades e fluxos estabelecidos no Plano de Recuperação de Desastres – DRP (Anexo III), sem prejuízo da adoção de procedimentos técnicos complementares definidos pelo Departamento de Tecnologia da Informação.

Art. 25 - Os procedimentos técnicos de contingência poderão abranger, entre outros, ações relativas a:
I - servidores de arquivos e de aplicações;
II - serviços de correio eletrônico;
III - acesso à internet e conectividade;
IV - rotinas de cópia de segurança e restauração; e
V - validação da integridade das informações recuperadas.

Parágrafo único - Os procedimentos técnicos referidos no *caput* poderão constar de manuais, planos operacionais ou documentos técnicos específicos, mantidos e atualizados pelo Departamento de Tecnologia da Informação, observadas as diretrizes da Política de Segurança da Informação e do DRP.

Art. 26 - Identificada a ocorrência de incidente grave ou situação de contingência, deverão ser adotadas as providências de comunicação, registro, acionamento técnico e recuperação previstas no Plano de Recuperação de Desastres – DRP (Anexo III).

Art. 27 - As ações de contingência e recuperação executadas deverão ser devidamente registradas, com indicação das medidas adotadas, dos responsáveis, dos prazos e dos resultados obtidos, para fins de controle, melhoria contínua e atendimento às auditorias.

Art. 28 - A revisão dos procedimentos de contingência deverá ocorrer sempre que houverem alterações relevantes no ambiente tecnológico ou institucional, ou em consonância com a revisão do Plano de Recuperação de Desastres – DRP e da Política de Segurança da Informação.

Parágrafo único - Os procedimentos de contingência referidos neste Capítulo não substituem o Plano de Recuperação de Desastres – DRP (Anexo III), que constitui o instrumento normativo central para fins de continuidade de serviços, testes periódicos e evidências institucionais.

CAPÍTULO XII
DA GESTÃO DE SEGURANÇA DA INFORMAÇÃO

Art. 29 - A Gestão de Segurança da Informação – GSI tem por finalidade coordenar, monitorar e promover as ações de segurança da informação no âmbito do Fundo de Aposentadorias e Pensões dos Servidores Públicos Municipais de Toledo – FAPES/TOLEDOPREV.

Art. 30 - A Gestão de Segurança da Informação será exercida por servidor a ser formalmente designado por ato do Chefe do Poder Executivo, preferencialmente integrante do quadro do Departamento de Tecnologia da Informação, considerando que o TOLEDOPREV não possui estrutura própria de tecnologia da informação.

Parágrafo único - Na impossibilidade de designação de servidor integrante do quadro do Departamento de Tecnologia da Informação, a função poderá ser exercida por servidor do TOLEDOPREV designado para tal finalidade, com apoio técnico do Departamento de Tecnologia da Informação, no que couber.

Art. 31 - Compete ao responsável pela Gestão de Segurança da Informação, no mínimo:
I - acompanhar a implementação da Política de Segurança da Informação e de seus Anexos;
II - promover ações de divulgação, orientação e conscientização em segurança da informação;
III - acompanhar, registrar e apoiar o tratamento de incidentes de segurança da informação, em articulação com o Departamento de Tecnologia da Informação, quando necessário;
IV - apoiar a realização das auditorias de acesso à informação, nos termos do Anexo IV;
V - apoiar a implementação, manutenção e revisão da Política de Classificação da Informação e dos respectivos registros de classificação, nos termos do Anexo II;
VI - apoiar a implementação, revisão e testes do Plano de Recuperação de Desastres – DRP, nos termos do Anexo III;

VII - propor iniciativas de melhoria contínua relacionadas à segurança da informação no âmbito do TOLEDOPREV;
VIII - consolidar, organizar e manter arquivadas as evidências e relatórios relacionados à segurança da informação (auditorias, testes do DRP, capacitações e demais registros), para fins de controle interno e certificação institucional; e
IX - atuar de forma integrada com a Coordenação do TOLEDOPREV e com o Departamento de Tecnologia da Informação.

CAPÍTULO XIII
DO COMITÊ DE SEGURANÇA DA INFORMAÇÃO

Art. 32 - O Comitê de Segurança da Informação – CSI será instituído por ato do Chefe do Poder Executivo, como instância colegiada de caráter consultivo e de apoio à governança da segurança da informação no âmbito do TOLEDOPREV.

Art. 33 - O Comitê de Segurança da Informação será composto por representantes:
I - do TOLEDOPREV;
II - do Departamento de Tecnologia da Informação; e
III - da Procuradoria-Geral do Município.

Art. 34 - Compete ao Comitê de Segurança da Informação – CSI:
I - acompanhar e avaliar a execução da Política de Segurança da Informação;
II - propor revisões e atualizações desta Política;
III - acompanhar a gestão de incidentes relevantes;
IV - acompanhar auditorias de acesso e testes do Plano de Recuperação de Desastres; e
V - promover a integração das ações de segurança da informação entre o TOLEDOPREV e o ente federativo.

Parágrafo único - As competências do Comitê de Segurança da Informação serão exercidas nos termos desta Política e detalhadas no Regimento Interno do CSI, homologado por Portaria Prefeito.

CAPÍTULO XIV
DA CLASSIFICAÇÃO DA INFORMAÇÃO

Art. 35 - As informações produzidas, recebidas ou custodiadas pelo TOLEDOPREV serão classificadas quanto ao grau de sigilo, nos termos do Anexo II – Política de Classificação da Informação.

Art. 36 - A classificação da informação observará o princípio da necessidade de conhecimento e a legislação aplicável, especialmente a Lei de Acesso à Informação e a Lei Geral de Proteção de Dados Pessoais.

CAPÍTULO XV
DA AUDITORIA DE ACESSOS À INFORMAÇÃO

Art. 37 - O acesso físico e lógico aos sistemas e às informações do TOLEDOPREV será objeto de auditoria periódica.

Art. 38 - A auditoria de acessos será realizada, no mínimo, uma vez ao ano, devendo gerar relatório formal.

Art. 39 - Os relatórios de auditoria deverão ser apresentados ao Comitê de Segurança da Informação, após sua instituição.

CAPÍTULO XVI
DA RECUPERAÇÃO DE DESASTRES

Art. 40 - O Fundo de Aposentadorias e Pensões dos Servidores Públicos Municipais de Toledo – FAPES/TOLEDOPREV manterá Plano de Recuperação de Desastres – DRP, instituído como Anexo III desta Política, com o objetivo de restabelecer, em tempo adequado, os serviços e sistemas críticos em caso de incidente grave ou desastre.

Art. 41 - O Plano de Recuperação de Desastres – DRP deverá definir, no mínimo:
I - o Tempo Objetivo de Recuperação – RTO;
II - o Ponto Objetivo de Recuperação – RPO;
III - os procedimentos de acionamento, recuperação e validação; e
IV - a realização de testes periódicos, com registro formal de seus resultados.

Parágrafo único - Os registros decorrentes da execução e dos testes do DRP constituem evidência para fins de controle interno, auditoria e certificação institucional, nos termos do Pró-Gestão RPPS.

CAPÍTULO XVII
DAS PENALIDADES

Art. 42 - O não cumprimento dos preceitos da Política de Segurança da Informação implicará a adoção das providências necessárias, mediante provocação ou de ofício, com vistas à aplicação das sanções administrativas cabíveis, especialmente as previstas no Estatuto dos Servidores Públicos Municipais de Toledo, observados o contraditório e a ampla defesa, sob pena de nulidade, sem prejuízo das demais sanções cíveis e penais previstas na legislação em vigor.

CAPÍTULO XVIII
DAS DISPOSIÇÕES FINAIS

Art. 43 - As disposições contidas no presente instrumento são de aplicação obrigatória, prevalecendo em qualquer hipótese e de acordo com os deveres e proibições legais e regulamentares.

Art. 44 - Todos os usuários ficam cientes de que os ambientes, sistemas, computadores e redes do TOLEDOPREV poderão ser monitorados e gravados.

Art. 45 - É vedado aos usuários de sistemas e serviços de informação do TOLEDOPREV aceitar ajuda técnica de pessoas estranhas e não autorizadas, salvo do quadro de servidores do Departamento de Tecnologia da Informação ou da equipe técnica especializada contratada mediante procedimento licitatório adequado.

Art. 46 - Fica vedada a divulgação ou reprodução de informações produzidas ou recebidas como resultado de atividade com o TOLEDOPREV, sem a autorização da Coordenação do TOLEDOPREV.

Art. 47 - Os usuários deverão ser cientificados da existência da Política de Segurança da Informação e sobre o uso correto dos ativos disponibilizados ao estabelecerem vínculo com o TOLEDOPREV, de forma a minimizar os possíveis riscos de segurança, bem como garantir o conhecimento de suas responsabilidades.

Art. 48 - O TOLEDOPREV exime-se de toda e qualquer responsabilidade decorrente do uso indevido, negligente ou imprudente dos recursos, serviços e informações, reservando-se o direito de analisar dados e evidências para obtenção de provas a serem utilizadas em processos investigatórios, bem como adotar as medidas legais cabíveis.

Parágrafo único - O usuário que tomar conhecimento de qualquer irregularidade relacionada à Política de Segurança da Informação contida neste instrumento deverá comunicar, imediatamente, a Coordenação do TOLEDOPREV.

Art. 49 – O TOLEDOPREV realizará, sempre que julgar necessário, ações preventivas e educativas visando a garantir a aplicação da Política de Segurança da Informação.

Art. 50 - Esta Política de Segurança da Informação poderá ser alterada mediante análise prévia do Conselho de Administração, considerando-se aprovada qualquer modificação pelo voto favorável da maioria absoluta dos conselheiros.

Art. 51 - O TOLEDOPREV terá o prazo de 60 (sessenta) dias para a adequação dos procedimentos, de acordo com o estabelecido neste instrumento, a partir da sua entrada em vigor.

§ 1º - No prazo previsto no *caput*, deverão ser editados os atos de designação do Responsável pela Gestão de Segurança da Informação – GSI e de instituição e nomeação dos membros do Comitê de Segurança da Informação – CSI, para plena execução desta Política e de seus Anexos.

§ 2º - Até a conclusão das providências previstas no § 1º, as atividades de coordenação necessárias à implementação inicial desta Política serão conduzidas pela autoridade competente no âmbito do TOLEDOPREV, com apoio técnico do Departamento de Tecnologia da Informação, no que couber.

Toledo, 27 de fevereiro de 2026.

ROSELI FABRIS DALLA COSTA
Diretora-Executiva/Coordenadora do TOLEDOPREV

LEANDRO MARCELO LUDVIG
Presidente do Conselho de Administração

ANEXO II
POLÍTICA DE CLASSIFICAÇÃO DA INFORMAÇÃO

CAPÍTULO I
DAS DISPOSIÇÕES GERAIS

Art. 1º - Esta Política de Classificação da Informação estabelece critérios e diretrizes para a classificação das informações produzidas, recebidas ou custodiadas pelo Fundo de Aposentadorias e Pensões dos Servidores Públicos Municipais de Toledo – FAPES/TOLEDOPREV, quanto ao grau de sigilo e às condições de acesso.

Art. 2º - A classificação da informação tem por finalidade assegurar a adequada proteção das informações, observados os princípios da confidencialidade, integridade e disponibilidade, bem como o atendimento à legislação vigente.

Art. 3º - Esta Política aplica-se às pessoas abrangidas pela Política de Segurança da Informação do TOLEDOPREV, que tenham acesso, a qualquer título, às informações, sistemas e ativos informacionais do TOLEDOPREV.

CAPÍTULO II
OS CRITÉRIOS DE CLASSIFICAÇÃO

Art. 4º - As informações do TOLEDOPREV serão classificadas considerando, entre outros, os seguintes critérios:
I - o impacto da divulgação não autorizada;
II - o grau de sensibilidade da informação;
III - as exigências legais e regulamentares; e
IV - a necessidade de restrição de acesso para o desempenho das atividades institucionais.

Art. 5º - Para fins desta Política, quando da utilização do Sistema Eletrônico de Informações – SEI, considera-se:
I - Nível de Acesso no SEI: marcação atribuída a processos e documentos para controle de visualização e pesquisa, podendo ser Público, Restrito–Unidade ou Restrito–Usuário;
II - Hipótese legal: fundamento normativo selecionado no SEI para justificar a restrição de acesso, conforme guia/tabela de hipóteses adotada pelo Município;
III - Restrito–Unidade: nível de acesso limitado aos usuários das unidades em que o processo tenha sido gerado ou por onde tenha tramitado; e
IV - Restrito–Usuário: nível de acesso limitado aos usuários com credencial de acesso específica no SEI.

CAPÍTULO III
DOS NÍVEIS DE CLASSIFICAÇÃO DA INFORMAÇÃO

Art. 6º - As informações serão classificadas nos seguintes níveis:
I - Informação Pública: aquela cujo acesso é livre, nos termos da legislação aplicável, não causando prejuízo ao TOLEDOPREV ou a terceiros quando divulgada;
II - Informação Restrita: aquela cujo acesso é limitado aos agentes públicos e colaboradores que necessitem conhecê-la para o desempenho de suas atividades;
III - Informação Confidencial: aquela cujo acesso é limitado a pessoas expressamente autorizadas, cuja divulgação indevida possa causar prejuízo institucional, administrativo ou financeiro; e

IV - Informação Sigilosa: aquela protegida por sigilo legal ou cuja divulgação não autorizada possa causar danos relevantes ao TOLEDOPREV, aos segurados, beneficiários ou a terceiros.

§ 1º - Para fins de operacionalização no SEI, a classificação prevista neste artigo deverá ser registrada mediante:
I - definição do Nível de Acesso (Público/Restrito–Unidade/Restrito–Usuário); e
II - indicação da hipótese legal correspondente, conforme guia/tabela adotada pelo Município.

§ 2º - Como regra geral, para fins de operacionalização no SEI, consideram-se:
I - Informações Públicas: Nível de acesso Público;
II - Informações Restritas e Confidenciais: Nível de acesso Restrito–Unidade; e
III - Informações que contenham dados pessoais sensíveis ou outras hipóteses que exijam limitação individualizada: Nível de acesso Restrito–Usuário.

CAPÍTULO IV
DO ACESSO À INFORMAÇÃO

Art. 7º - O acesso às informações observará o nível de classificação atribuído e o princípio da necessidade de conhecimento.

Art. 8º - A concessão, a alteração ou a revogação de acesso às informações deverá ser compatível com as atribuições do usuário e com as normas estabelecidas na Política de Segurança da Informação – PSI.

Art. 9º - No âmbito do SEI, os processos e documentos deverão, em regra, possuir nível de acesso Público e, excepcionalmente, nível de acesso Restrito, com a indicação da hipótese legal aplicável, nos termos do guia/tabela de hipóteses adotada pelo Município.

§ 1º - A restrição de acesso deverá ser atribuída preferencialmente aos documentos, mantido o processo com nível de acesso público.

§ 2º - Excepcionalmente, durante a tramitação de procedimentos em que a publicidade possa prejudicar sua adequada conclusão, o processo poderá receber nível de acesso Restrito–Unidade, mediante hipótese legal correspondente a documento preparatório, devendo, ao final, ter seu nível de acesso alterado para Público, mantidas as restrições cabíveis aos documentos individualmente considerados.

§ 3º - É vedada a atribuição de restrição a documentos com fundamento genérico de “documento preparatório”, devendo cada documento receber nível de acesso e hipótese legal conforme o teor da informação nele contida.

CAPÍTULO V
DA CLASSIFICAÇÃO E DA RESPONSABILIDADE

Art. 10 - Compete ao TOLEDOPREV, por meio de suas áreas responsáveis, classificar as informações sob sua guarda, com apoio e orientações da Gestão de Segurança da Informação – GSI.

Art. 11 - Os usuários são responsáveis por respeitar a classificação atribuída às informações às quais tenham acesso, observando as regras de acesso, uso,

armazenamento e tratamento previstas nesta Política, sendo vedada sua divulgação, reprodução, extração, compartilhamento ou qualquer outra forma de disponibilização em desacordo com o nível de classificação atribuído.

Parágrafo único - O descumprimento do disposto neste artigo sujeitará o responsável às medidas administrativas cabíveis e às demais responsabilizações previstas na Política de Segurança da Informação do TOLEDOPREV (Anexo I), sem prejuízo das demais sanções legais aplicáveis.

Art. 12 - A classificação atribuída deverá ser registrada de forma identificável, contendo, no mínimo, o nível de classificação, a data e a unidade responsável pela atribuição, podendo ser mantida em controle administrativo próprio.

§ 1º - O controle administrativo referido no *caput* deverá ser mantido de forma organizada e disponível para auditoria interna, observadas as regras de acesso, sigilo e proteção de dados aplicáveis.

§ 2º - A gestão e a guarda dos registros de classificação observarão, quando aplicável, os prazos de guarda e a temporalidade estabelecidos nas normas internas de gestão documental e arquivística adotadas no âmbito do Município.

§ 3º - A Gestão de Segurança da Informação – GSI prestará orientação às áreas responsáveis quanto ao registro da classificação e apoiará a organização e a manutenção do controle administrativo referido neste artigo, sem prejuízo das responsabilidades das unidades classificadoras.

CAPÍTULO VI
DA TEMPORALIDADE E GUARDA DA INFORMAÇÃO

Art. 13 - A classificação da informação deverá considerar a temporalidade de guarda, observadas as normas arquivísticas e a legislação aplicável.

Art. 14 - Decorrido o prazo de guarda ou cessada a necessidade de restrição, a informação poderá ter sua classificação revista, conforme avaliação da área responsável.

CAPÍTULO VII
DA REVISÃO DA CLASSIFICAÇÃO

Art. 15 - A classificação da informação poderá ser revista sempre que houver alteração em seu conteúdo, finalidade ou grau de sensibilidade.

Art. 16 - A revisão da classificação deverá observar as orientações da Gestão de Segurança da Informação – GSI e, quando couber, após instituído o Comitê de Segurança da Informação – CSI, ser comunicada ao referido Comitê.

CAPÍTULO VIII
DAS DISPOSIÇÕES FINAIS

Art. 17 - O descumprimento desta Política sujeitará os responsáveis às sanções administrativas cabíveis, nos termos da legislação vigente e da Política de Segurança da Informação.

Art. 18 - As hipóteses de restrição de acesso no SEI referem-se às limitações de acesso previstas em lei (informação pessoal, informação pessoal sensível, sigilos legais e documentos preparatórios), não se confundindo com a classificação em grau de sigilo reservado, secreto ou ultrassecreto prevista na Lei nº 12.527/2011, cujo tratamento observará normativos específicos, quando aplicável.

Toledo, 27 de fevereiro de 2026.

ROSELI FABRIS DALLA COSTA
Diretora-Executiva/Coordenadora do TOLEDOPREV

LEANDRO MARCELO LUDVIG
Presidente do Conselho de Administração

ANEXO III
PLANO DE RECUPERAÇÃO DE DESASTRES – DRP

CAPÍTULO I
DO OBJETIVO E DA ABRANGÊNCIA

Art. 1º - O presente Plano de Recuperação de Desastres – DRP estabelece diretrizes e procedimentos para recuperação dos serviços e sistemas críticos utilizados pelo FAPES/TOLEDOPREV em caso de incidente grave ou desastre, assegurando a continuidade das atividades essenciais.

Art. 2º - O DRP aplica-se aos sistemas, bases de dados, informações, equipamentos e serviços tecnológicos utilizados pelo TOLEDOPREV, bem como aos usuários envolvidos em sua operação, observadas as responsabilidades definidas neste Plano.

CAPÍTULO II
DAS DEFINIÇÕES

Art. 3º - Para fins deste Plano, considera-se:
I - Incidente Grave: evento que comprometa significativamente a disponibilidade, integridade ou confidencialidade das informações ou sistemas;
II - Desastre: evento que provoque interrupção prolongada ou indisponibilidade total de sistemas e serviços críticos;
III - RTO (Tempo Objetivo de Recuperação): tempo máximo aceitável para o restabelecimento do serviço após incidente grave ou desastre; e
IV - RPO (Ponto Objetivo de Recuperação): limite máximo de perda de dados aceitável, medido em tempo, a partir do último backup válido.

CAPÍTULO III
DAS RESPONSABILIDADES

Art. 4º - Compete ao Responsável pela Gestão de Segurança da Informação – GSI, a ser designado na forma do Anexo I – PSI:
I - coordenar a ativação e a condução deste Plano;
II - registrar o incidente e promover a comunicação institucional necessária;
III - articular a execução técnica com o Departamento de Tecnologia da Informação;
IV - consolidar e arquivar os registros e relatórios decorrentes da execução e dos testes do DRP; e
V - após instituído o Comitê de Segurança da Informação – CSI, submeter ao referido Comitê as informações relevantes e os resultados de testes.

Art. 5º - Compete ao Departamento de Tecnologia da Informação:
I - executar os procedimentos técnicos de recuperação, restauração e validação;
II - assegurar a disponibilidade dos backups e dos recursos necessários à recuperação; e
III - apoiar a verificação de integridade dos dados restaurados.

Art. 6º - Compete ao Comitê de Segurança da Informação – CSI, após sua instituição, acompanhar a aplicação deste Plano, avaliando resultados de testes e propondo melhorias.

CAPÍTULO IV
DOS SISTEMAS E SERVIÇOS CRÍTICOS

Art. 7º - Para fins deste Plano, são considerados sistemas e serviços críticos do TOLEDOPREV, no mínimo:
I - sistema previdenciário;
II - sistema de folha de pagamento de benefícios;
III - bases de dados previdenciárias e cadastrais;
IV - sistemas administrativos essenciais; e
V - site institucional.

Parágrafo único - A relação de sistemas críticos poderá ser ajustada pela Gestão de Segurança da Informação, com ciência do CSI, após sua instituição, sempre que houver alteração relevante no ambiente tecnológico ou institucional.

CAPÍTULO V
DOS PARÂMETROS DE RECUPERAÇÃO (RTO e RPO)

Art. 8º - Ficam definidos os seguintes parâmetros mínimos de recuperação:

Sistema / Serviço	RTO	RPO
Sistema previdenciário	até 24 horas	até 24 horas
Folha de pagamento de benefícios	até 24 horas	até 24 horas
Bases de dados previdenciárias	até 24 horas	até 24 horas
Sistemas administrativos essenciais	até 48 horas	até 24 horas
Site institucional	até 48 horas	até 24 horas

CAPÍTULO VI
DO ACIONAMENTO E DOS PROCEDIMENTOS DE RECUPERAÇÃO

Art. 9º - Identificado incidente grave ou desastre, deverão ser adotadas as seguintes providências mínimas:
I - registro do incidente (data, horário, descrição e impacto);
II - comunicação imediata ao Responsável pela GSI;
III - acionamento do Departamento de Tecnologia da Informação, com definição da prioridade;
IV - avaliação do impacto e definição da estratégia de recuperação;
V - execução da restauração dos sistemas e dados, a partir de backups válidos; e
VI - validação do restabelecimento dos serviços e verificação de integridade.

Art. 10 - A restauração deverá observar os parâmetros de RTO e RPO definidos no art. 8º, sem prejuízo de medidas emergenciais para continuidade de serviços essenciais.

CAPÍTULO VII
DE BACKUP, RESTAURAÇÃO E VALIDAÇÃO

Art. 11 - Os procedimentos de backup observarão as normas internas vigentes, especialmente o Manual de Cópias de Segurança do FAPES/TOLEDOPREV, devendo sua execução técnica ocorrer com apoio do Departamento de Tecnologia da Informação do Município de Toledo, quando necessário, sem prejuízo das responsabilidades definidas neste Plano.

Art. 12 - Após a recuperação, deverá ser realizada validação mínima do funcionamento dos sistemas e consistência dos dados restaurados, registrando-se eventuais divergências e providências adotadas.

CAPÍTULO VIII
DOS TESTES PERIÓDICOS E REGISTROS

Art. 13 - O DRP deverá ser testado, no mínimo, uma vez ao ano, mediante procedimento de simulação e/ou restauração controlada, conforme viabilidade técnica.

Art. 14 - O teste do DRP deverá gerar Relatório de Teste, contendo, no mínimo:
I - data do teste;
II - sistemas testados;
III - tempo observado de recuperação;
IV - aderência a RTO e RPO;
V - falhas identificadas e ações corretivas propostas; e
VI - assinaturas do Responsável pela GSI e do responsável técnico da TI do Município, com ciência do CSI.

Parágrafo único - O Relatório de Teste referido no *caput* deverá ser arquivado em controle administrativo próprio e permanecer disponível para auditoria interna, para fins de controle e certificação institucional.

CAPÍTULO IX
DA ATUALIZAÇÃO DO PLANO

Art. 15 - Este Plano deverá ser atualizado sempre que houver alterações relevantes no ambiente tecnológico ou institucional e, quando couber, em consonância com o processo de revisão da Política de Segurança da Informação.

Toledo, 27 de fevereiro de 2026.

ROSELI FABRIS DALLA COSTA
Diretora-Executiva/Coordenadora do TOLEDOPREV

LEANDRO MARCELO LUDVIG
Presidente do Conselho de Administração

ANEXO IV
MANUAL DE AUDITORIA DE ACESSOS À INFORMAÇÃO

CAPÍTULO I
DO OBJETIVO

Art. 1º - Este Manual estabelece os procedimentos para a realização de auditorias periódicas dos acessos físicos e lógicos às informações e aos sistemas utilizados pelo Fundo de Aposentadorias e Pensões dos Servidores Públicos Municipais de Toledo – FAPES/TOLEDOPREV, com a finalidade de verificar a conformidade com a Política de Segurança da Informação – PSI.

CAPÍTULO II
DA ABRANGÊNCIA

Art. 2º - A auditoria de acessos abrange, no mínimo:
I - os sistemas informatizados utilizados pelo TOLEDOPREV;
II - as bases de dados previdenciárias, cadastrais e administrativas;
III - os perfis de acesso concedidos aos usuários; e
IV - os acessos realizados por servidores, colaboradores e prestadores de serviços.

CAPÍTULO III
DAS RESPONSABILIDADES

Art. 3º - Compete ao Responsável pela Gestão de Segurança da Informação – GSI, a ser designado nos termos do Anexo I – PSI, no que couber:
I - planejar e coordenar a auditoria de acessos;
II - solicitar o apoio técnico necessário ao Departamento de Tecnologia da Informação;
III - analisar os resultados da auditoria;
IV - consolidar e arquivar os relatórios de auditoria; e
V - após instituído o Comitê de Segurança da Informação – CSI, submeter os resultados ao referido Comitê.

Art. 4º - Compete ao Departamento de Tecnologia da Informação:
I - fornecer as informações técnicas necessárias à auditoria;
II - apoiar a extração de registros de acesso; e
III - executar ajustes técnicos quando demandados.

Art. 5º - Compete ao Comitê de Segurança da Informação – CSI, após sua instituição, acompanhar os resultados das auditorias e propor medidas de melhoria.

CAPÍTULO IV
DA PERIODICIDADE

Art. 6º - A auditoria de acessos deverá ser realizada, no mínimo, uma vez ao ano, ou sempre que identificado incidente relevante de segurança da informação.

Parágrafo único - Auditorias extraordinárias poderão ser realizadas por determinação da Gestão de Segurança da Informação e, após instituído o CSI, por deliberação do referido Comitê.

CAPÍTULO V
DOS PROCEDIMENTOS DE AUDITORIA

Art. 7º - A auditoria de acessos deverá contemplar, no mínimo:
I - verificação de usuários ativos e inativos;
II - verificação da compatibilidade entre os perfis de acesso e as atribuições funcionais;
III - identificação de acessos indevidos ou excessivos;
IV - verificação de acessos de usuários desligados, cedidos ou com alteração de função; e
V - verificação do cumprimento da Política de Classificação da Informação.

Art. 8º - Sempre que possível, a auditoria deverá utilizar registros de logs, relatórios de sistemas ou outros mecanismos de controle disponíveis.

CAPÍTULO VI
DO RELATÓRIO DE AUDITORIA

Art. 9º - A auditoria de acessos deverá resultar em Relatório de Auditoria, contendo, no mínimo:
I - período auditado;
II - sistemas e informações analisados;
III - metodologia adotada;
IV - achados identificados;
V - não conformidades verificadas, quando houver;
VI - recomendações ou ações corretivas propostas;
VII - responsáveis pelas providências e prazos sugeridos, quando aplicável; e
VIII - encaminhamentos adotados.

Art. 10 - O Relatório de Auditoria deverá ser assinado pelo Responsável pela GSI e conter a ciência do responsável técnico da área de Tecnologia da Informação do Município de Toledo.

CAPÍTULO VII
DAS PROVIDÊNCIAS E ACOMPANHAMENTO

Art. 11 - As não conformidades identificadas deverão ser objeto de providências corretivas, acompanhadas pela Gestão de Segurança da Informação.

Art. 12 - O Comitê de Segurança da Informação – CSI, após sua instituição, deverá acompanhar a implementação das providências recomendadas e avaliar a necessidade de ajustes na Política de Segurança da Informação ou em seus anexos.

CAPÍTULO VIII
DO ARQUIVAMENTO E DA EVIDÊNCIA

Art. 13 - Os Relatórios de Auditoria de Acessos deverão ser arquivados em meio físico ou digital, de forma organizada e identificável, constituindo evidência para fins de controle interno e de certificação institucional, devendo permanecer disponível para auditoria interna.

Toledo, 27 de fevereiro de 2026.

ROSELI FABRIS DALLA COSTA
Diretora-Executiva/Coordenadora do TOLEDOPREV

LEANDRO MARCELO LUDVIG
Presidente do Conselho de Administração

ANEXO V
PLANO ANUAL DE CAPACITAÇÃO EM SEGURANÇA DA INFORMAÇÃO

CAPÍTULO I
DO OBJETIVO

Art. 1º - Este Plano Anual de Capacitação em Segurança da Informação tem por objetivo promover a conscientização e o aprimoramento dos conhecimentos dos usuários quanto às diretrizes e procedimentos de segurança da informação adotados pelo Fundo de Aposentadorias e Pensões dos Servidores Públicos Municipais de Toledo – FAPES/TOLEDOPREV, em consonância com a Política de Segurança da Informação – PSI.

CAPÍTULO II
DA ABRANGÊNCIA E DO PÚBLICO-ALVO

Art. 2º - O Plano aplica-se às pessoas abrangidas pela Política de Segurança da Informação do TOLEDOPREV (Anexo I) que tenham acesso às informações, sistemas ou recursos tecnológicos utilizados pelo TOLEDOPREV, incluindo agentes públicos, conselheiros, colaboradores, estagiários e prestadores de serviços.

Art. 3º - A participação nas ações de capacitação será obrigatória para os usuários que, em razão de suas atribuições, tenham acesso a informações classificadas como Restritas, Confidenciais ou Sigilosas.

CAPÍTULO III
DOS CONTEÚDOS MÍNIMOS

Art. 4º - As ações de capacitação em segurança da informação deverão contemplar, no mínimo, os seguintes conteúdos:
I - princípios da segurança da informação (confidencialidade, integridade e disponibilidade);
II - diretrizes da Política de Segurança da Informação – PSI;
III - Política de Classificação da Informação;
IV - boas práticas de uso de sistemas, correio eletrônico e internet;
V - proteção de dados pessoais e noções gerais da Lei Geral de Proteção de Dados Pessoais – LGPD; e
VI - procedimentos básicos de prevenção e comunicação de incidentes de segurança da informação.

CAPÍTULO IV
DA PERIODICIDADE E DAS FORMAS DE CAPACITAÇÃO

Art. 5º - As ações de capacitação em segurança da informação deverão ser realizadas, no mínimo, uma vez ao ano.

Art. 6º - As capacitações poderão ser realizadas por meio de:
I - treinamentos presenciais;
II - capacitações remotas ou virtuais;
III - palestras, oficinas ou reuniões orientativas; e
IV - materiais informativos, comunicados ou campanhas internas.

Parágrafo único - Sempre que possível, as ações de capacitação poderão contar com o apoio técnico do Departamento de Tecnologia da Informação.

CAPÍTULO V
DAS RESPONSABILIDADES

Art. 7º - Compete ao Responsável pela Gestão de Segurança da Informação – GSI, a ser designado nos termos do Anexo I – PSI, no que couber:
I - planejar e coordenar a execução das ações de capacitação;
II - após instituído o Comitê de Segurança da Informação – CSI, definir, em conjunto com o referido Comitê, os temas prioritários; e
III - registrar e arquivar as evidências das capacitações realizadas.

Art. 8º - Compete ao Comitê de Segurança da Informação – CSI, após sua instituição, acompanhar a execução do Plano e propor melhorias nas ações de capacitação.

CAPÍTULO VI
DOS REGISTROS E DAS EVIDÊNCIAS

Art. 9º - As ações de capacitação deverão ser registradas por meio de, no mínimo:
I - lista de presença, quando presencial;
II - registro de participação, quando remoto;
III - material didático ou informativo utilizado; e
IV - relatório sintético da ação realizada.

Art. 10 - Os registros de capacitação constituem evidência para fins de controle interno e de certificação institucional, devendo ser mantidos de forma organizada e disponíveis para auditoria interna.

CAPÍTULO VII
DA AVALIAÇÃO E DA ATUALIZAÇÃO DO PLANO

Art. 11 - O Plano Anual de Capacitação em Segurança da Informação deverá ser avaliado periodicamente pela Gestão de Segurança da Informação, considerando os resultados das auditorias, dos incidentes registrados, dos testes do Plano de Recuperação de Desastres – DRP, e das necessidades institucionais.

Art. 12 - O Plano poderá ser ajustado sempre que necessário, observadas as diretrizes da Política de Segurança da Informação.

Toledo, 27 de fevereiro de 2026.

ROSELI FABRIS DALLA COSTA
Diretora-Executiva/Coordenadora do TOLEDOPREV

LEANDRO MARCELO LUDVIG
Presidente do Conselho de Administração