POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

2025

1. ESCOPO:

1.1. OBJETIVO

A Política de Segurança da Informação (PSI) tem por objetivo a instituição de diretrizes estratégicas que visam garantir a disponibilidade, integridade, confidencialidade e autenticidade das informações, bem como atitudes adequadas para manuseio, tratamento, controle e proteção dos dados, informações, documentos e conhecimentos produzidos, armazenados, sob guarda ou transmitidos por qualquer meio ou recurso do Instituto de Previdência dos Servidores Públicos do Município de Duas Barras - PREVDB contra ameaças e vulnerabilidades. Desse modo, a Política busca preservar os seus ativos de informação, assim como a sua imagem institucional.

O propósito da Política é orientar o PREVDB no que diz respeito à gestão de riscos e ao tratamento de incidentes de Segurança da Informação (SIN), em conformidade com as disposições constitucionais, legais e regimentais vigentes.

A PSI estabelece o comprometimento da alta direção organizacional do Instituto, com vistas a prover apoio para a implantação da Gestão dos Riscos de Segurança da Informação (GRSIN).

1.2. ABRANGÊNCIA

Esta PSI aplica-se à Sede do PREVDB, sendo de responsabilidade de todos os servidores, colaboradores internos ou externos, devendo ser dado amplo conhecimento de seu teor a todas as pessoas ou organizações que utilizam os meios físicos ou lógicos do PREVDB, por serem todos responsáveis por garantir a segurança das informações a que tenham acesso.

2. CONCEITOS E DEFINIÇÕES:

Para os efeitos desta PSI, são estabelecidos os seguintes conceitos e definições:

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. Ameaça: qualquer evento que explore vulnerabilidades ou seja causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização;

III. Análise de Riscos: uso sistemático de informações para identificar fontes e avaliar riscos;

IV. Análise/Avaliação de Riscos: processo completo de análise e avaliação de riscos;

V. Atividade: processo ou conjunto de processos executados por um órgão ou entidade, ou em seu nome, que produzem ou suportem um ou mais produtos ou serviços;

VI. Ativo: qualquer componente (seja humano, tecnológico, software ou outros) que sustente uma ou mais atividades e que tenha valor para a organização;

VII. Ativos de Informação: os meios de armazenamento, transmissão e processamento; os sistemas de informação; além das informações em si, bem como os locais em que se encontram esses meios e as pessoas que têm acesso a eles;

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

IX. Avaliação de Riscos: processo de comparar o risco estimado com critérios predefinidos para determinar a importância do risco;

X. Celeridade: as ações de segurança da informação e comunicações devem oferecer respostas rápidas a incidentes e falhas;

XI. Classificação da Informação: identificação dos níveis de proteção que as informações demandam; atribuição de classes e formas de identificação, além de determinação dos controles de proteção necessários a cada uma delas;

XII. Comunicação do Risco: troca ou compartilhamento de informação sobre o risco entre o tomador de decisão e outras partes interessadas;

XIII. Confidencialidade: propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizada ou não credenciada;

XIV. Controle de Acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso;

XV. Custodiante do Ativo de Informação: é aquele que, de alguma forma, zela pelo armazenamento, operação, administração e preservação de ativos de informação que não lhe pertencem, mas que estão sob sua custódia;

XVI. Desastre: evento repentino e não planejado que causa perda para toda ou parte da organização, com sérios impactos em sua capacidade de prestar serviços essenciais ou críticos, por um período superior ao prazo de recuperação;

XVII. Descarte: eliminação correta de informações, documentos, mídias e acervos digitais;

XVIII. Disponibilidade: propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade;

XIX. Estimativa de Riscos: processo utilizado para atribuir valores à probabilidade e consequências de determinado risco;

XX. Eficácia: realização de um trabalho que atinja os resultados esperados;

XXI. Eficiência: realização de um trabalho, com presteza, agilidade e eficácia;

XXII. Ética: preservação dos direitos dos agentes públicos, sem comprometimento da Segurança da Informação;

XXIII. Evento de Segurança da Informação: ocorrência identificada de procedimento, sistema, serviço ou rede que indica possível perda de controle ou violação da política de segurança da informação, ou situação desconhecida que possa ser relevante para a segurança da informação;

XXIV. Gerenciamento de Operações e Comunicações: atividades, processos, procedimentos e recursos que visam disponibilizar e manter serviços, sistemas e infraestrutura que os suportem;

XXV. Gestão de Ativos: processo de identificação dos ativos e de definição de responsabilidades pela manutenção apropriada de seu controle;

XXVI. Gestão de Riscos de Segurança da Informação: conjunto de processos que permitem identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos;

XXVII. Gestão de Segurança da Informação: ações e métodos que visam à integração das atividades de gestão de riscos, tratamento de incidentes, tratamento da informação, conformidade, credenciamento, segurança cibernética, segurança física, segurança lógica, segurança orgânica e segurança organizacional aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto, no âmbito da tecnologia da informação e comunicações;

XXVIII. Gestor de Segurança da Informação: é o servidor público responsável pelas ações de segurança da informação e comunicações do PREVDB;

XXIX. Identificação de Riscos: processo para localizar, listar e caracterizar elementos do risco;

XXX. Incidente de SIN: evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de computação ou de redes de computadores;

XXXI. Informação: conjunto de dados, textos, imagens, métodos, sistemas ou quaisquer formas de representação dotadas de significado em determinado contexto, independentemente do suporte em que resida ou da forma pela qual seja veiculado;

XXXII. Integridade: propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

XXXIII. Política de Segurança da Informação: documento aprovado pela autoridade responsável do PREVDB, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação e comunicações;

XXXIV. Proprietário de Ativos de Informação: unidade administrativa responsável por gerenciar determinado segmento de informação e todos os ativos relacionados;

XXXV. Quebra de Segurança: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e das comunicações;

XXXVI. Recursos Criptográficos: sistemas, programas, processos e equipamentos, isolados ou em rede, que utilizam algoritmo simétrico ou assimétrico, para realizar a cifração ou decifração de informações;

XXXVII. Resiliência: poder de recuperação ou capacidade de uma organização resistir aos efeitos de um desastre;

XXXVIII. Responsabilidade: dever dos agentes públicos em conhecer e respeitar todas as normas de segurança da informação e comunicações da respectiva instituição;

XXXIX. Risco de SIN: potencial associado à exploração de uma ou mais vulnerabilidades de um ativo de informação ou de um conjunto de ativos, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização;

XL. Segurança Física e do Ambiente: processo referente à proteção de todos os ativos físicos da instituição, englobando instalações físicas, internas e externas, em todas as localidades em que a organização estiver presente;

XLI. Sistema Estruturante: conjunto de sistemas informáticos fundamentais e imprescindíveis para a consecução das atividades administrativas, de forma eficaz e eficiente;

XLII. Terceiros: quaisquer pessoas, físicas ou jurídicas, de natureza pública ou privada, externos ao PREVDB;

XLIII. Transferir Risco: forma de tratamento de risco na qual a alta administração decide realizar a atividade, compartilhando com outra entidade o ônus associado a um risco;

XLIV. Tratamento da Informação: conjunto de ações referentes à recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação;

XLV. Tratamento de Incidentes: processo que consiste em receber, filtrar, classificar e responder às solicitações e alertas, bem como realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e a identificação de tendências potenciais futuras;

XLVI. Tratamento dos Riscos: processo e implementação de ações de segurança da informação e comunicações, com o objetivo de evitar, reduzir, reter ou transferir um risco;

XLVII. Usuário: agente público que obteve autorização do responsável pela área interessada para acesso aos ativos de informação;

XLVIII. Vulnerabilidade: conjunto de fatores internos ou causas potenciais de um incidente indesejado, que podem resultar em risco para um sistema ou organização, os quais devem ser evitados por ação interna de segurança da informação.

3. REFERÊNCIAS E NORMATIVAS:

I. Lei 8.159, de 8 de janeiro de 1991: dispõe sobre a Política Nacional de Arquivos Públicos e Privados e dá outras providências;

II. Lei nº 9.983, de 14 de julho de 2000: dispõe sobre a responsabilidade administrativa, civil e criminal de usuários que cometam irregularidades em razão do acesso a dados, informações e sistemas informatizados da Administração Pública;

III. Lei nº 12.527, de 18 de novembro de 2011: regulamenta o acesso às informações públicas;

IV. Decreto nº 3.505, de 13 de junho de 2000: institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal;

V. Decreto nº 5.482, de 30 de junho de 2005: dispõe sobre a divulgação de dados e informações pelos órgãos e entidades da Administração Pública Federal, por meio da Rede Mundial de Computadores – Internet;

VI. Decreto nº 7.845, de 14 de novembro de 2012: regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento;

VII. Decreto Nº 8.638, de 15 de janeiro de 2016: institui a Estratégia de Governança Digital;

VIII. Norma ABNT NBR ISO/IEC 27001:2013: estabelece os elementos de um Sistema de Gestão de Segurança da Informação e Comunicações;

IX. Norma ABNT NBR ISO/IEC 27002:2013: institui o código de melhores práticas para Gestão de Segurança da Informação e da Comunicação;

X. Norma ABNT NBR ISO/IEC 27005:2011: estabelece diretrizes para o processo de gestão de riscos de segurança da informação.

4. PRINCÍPIOS:

Esta Política de Segurança da Informação e suas ações serão norteadas pelos seguintes princípios:

I. Celeridade: as ações de SIN devem oferecer respostas rápidas a incidentes e falhas de segurança;

II. Ética: os direitos e interesses legítimos dos usuários e agentes públicos devem ser preservados, sem comprometimento da SIN;

III. Clareza: as regras de segurança dos ativos de SIN devem ser precisas, concisas e de fácil entendimento;

IV. Legalidade: as ações de segurança devem respeitar as atribuições regimentais, bem como as leis, normas e políticas organizacionais, administrativas, técnicas e operacionais do PREVDB;

V. Publicidade: transparência no trato da informação, observados os critérios legais.

5. DIRETRIZES GERAIS:

As diretrizes de segurança da informação estabelecidas nesta PSI aplicam-se às informações armazenadas, acessadas, produzidas e transmitidas pelo PREVDB, e que devem ser seguidas pelos usuários, incumbindo a todos a responsabilidade e o comprometimento com sua aplicação.

Independentemente da forma ou do meio pelo qual a informação seja apresentada ou compartilhada, deverá ser sempre protegida adequadamente, de acordo com esta Política.

Os recursos de Tecnologia da Informação (TIN) disponibilizados pelo PREVDB serão utilizados estritamente para propósito institucional.

É vedado a qualquer usuário do PREVDB o uso dos recursos de Tecnologia da Informação para fins pessoais (próprios ou de terceiros), entretenimento, veiculação de opiniões político-partidárias ou religiosas, bem como para perpetrar 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 instituição, comprometendo a integridade, a confidencialidade, a confiabilidade, autenticidade ou a disponibilidade das informações.

As diretrizes desta PSI constituem os principais pilares da Gestão de Segurança da Informação do PREVDB, sendo norteadoras da elaboração das normas de SIN.

Os casos omissos e as dúvidas decorrentes da aplicação do disposto nesta PSI, devem ser direcionados ao Gestor de Segurança da Informação (GSI).

6. DIRETIZES ESPECÍFICAS:

6.1. GESTÃO DA SEGURANÇA DA INFORMAÇÃO (GESIN):

Todos os mecanismos de proteção utilizados para a SIN devem ser mantidos com o objetivo de garantir a continuidade dos negócios do PREVDB.

As medidas de proteção devem ser planejadas e os gastos da aplicação de controles devem ser compatíveis com o valor do ativo protegido.

Os requisitos de segurança da informação e comunicações do PREVDB devem ser explicitamente citados em todos os termos de compromisso celebrados entre a instituição e terceiros, por meio de cláusula específica sobre a obrigatoriedade de atendimento às diretrizes desta Política, devendo também ser exigido termo de confidencialidade.

6.2. GESTÃO DE RISCOS E SEGURANÇA DA INFORMAÇÃO (GRSIN):

A GRSIN é um conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os ativos de informação do PREVDB, e equilibrá-los com os custos operacionais e financeiros envolvidos.

As áreas responsáveis por ativos de informação deverão implementar processo contínuo de Gestão de Riscos, que será aplicado na implementação e operação da GRSIN.

A GRSI deve ser implementada no âmbito do PREVDB, visando identificar os ativos relevantes e determinar ações de gestão apropriadas, devendo ser atualizada periodicamente, no mínimo 01 (uma) vez por ano, ou oportunamente, em função de inventários de ativos, mudanças, ameaças ou vulnerabilidades. Trata-se de instrumento do programa de Gestão de Riscos que deve incluir um Plano de Gerenciamento de Incidentes (PGI).

O Plano de Gerenciamento de Incidentes definirá responsabilidades e procedimentos para assegurar respostas rápidas, efetivas e ordenadas perante incidentes de SIN.

6.3. GESTÃO DE ATIVOS DE INFORMAÇÃO:

A gestão de ativos de informação do PREVDB deverá observar normas operacionais e procedimentos específicos para garantir a sua operação segura e contínua.

Os ativos de informação do Instituto deverão ser inventariados, com a classificação em termos de valor, requisitos legais, sensibilidade e criticidade da informação para o PREVDB, e serão atribuídos aos respectivos responsáveis. Seu uso deverá estar em conformidade com os princípios e normas operacionais de SIN, sendo destinados exclusivamente ao uso institucional, vedada a utilização para fins em desconformidade com os interesses do PREVDB.

O usuário deve ter acesso apenas aos ativos necessários e indispensáveis ao seu trabalho, respeitando as recomendações de sigilo, conforme disposto em normas e legislação específica de classificação de informação.

É vedado comprometer a integridade, a confidencialidade ou a disponibilidade das informações criadas, manuseadas, armazenadas, transportadas, descartadas ou custodiadas pelo PREVDB.

6.4. TRATAMENTO DA INFORMAÇÃO:

A informação deve ser protegida de forma preventiva, com o objetivo de minimizar riscos às atividades e serviços do PREVDB. Essa proteção deve ser de acordo com o valor, sensibilidade e criticidade da informação, devendo ser desenvolvido, para este fim, sistema de classificação da informação. Os dados, as informações e os sistemas de informação do PREVDB devem ser protegidos contra ameaças e ações não autorizadas, acidentais ou não, de modo a reduzir riscos e garantir a disponibilidade, integridade, confidencialidade e autenticidade desses bens.

6.5. CLASSIFICAÇÃO DA INFORMAÇÃO:

Toda informação criada, manuseada, armazenada, transportada ou descartada do PREVDB será classificada de acordo com a Lei nº 12.527, de 18 de novembro 2011.

O usuário deverá ser capaz de identificar a classificação atribuída a uma informação tratada pelo PREVDB e, a partir dela, conhecer e obedecer às restrições de acesso e divulgação associadas.

As informações sob gestão do PREVDB devem dispor de segurança, de maneira a serem adequadamente protegidas quanto ao acesso e uso. Para aquelas consideradas de alta criticidade, serão necessárias medidas especiais de tratamento, com o objetivo de limitar a exploração de informações exclusivas da instituição.

6.6. MONITORAMENTO, AUDITORIA E CONFORMIDADE:

O monitoramento, auditoria e conformidade de ativos de informações observarão o seguinte:

I. O uso dos recursos de tecnologia da informação e comunicações disponibilizados pelo PREVDB é passível de monitoramento e auditoria, devendo ser implementados e mantidos, à medida do possível, mecanismos que permitam a sua rastreabilidade;

II. A entrada e saída de ativos de informação do PREVDB deverá ser registrada e autorizada por autoridade competente mediante procedimento formal;

III. A Diretoria Financeira manterá registros e procedimentos específicos, tais como trilhas de auditoria e outros que assegurem o rastreamento, acompanhamento, controle e verificação de acessos a todos os sistemas institucionais, à rede interna e à internet;

IV. A Ouvidoria da PREVDB será responsável por manter canal de comunicação para recebimento de denúncias de infração a qualquer parte desta PSI.

6.7. CONTROLE DE ACESSO E USO DE SENHAS:

As regras de controle de acesso a todos os sistemas institucionais, intranet, internet, informações, dados e às instalações físicas do PREVDB deverão ser definidas e regulamentadas, por meio de normas internas, com o objetivo de garantir a segurança dos usuários e a proteção dos ativos da instituição.

6.8. USO DE E-MAIL:

O correio eletrônico é um recurso oficial de comunicação institucional do Instituto de Previdência dos Servidores Públicos do Município de Duas Barras – PREVDB. Para o desempenho de suas atividades administrativas e operacionais, o PREVDB disponibiliza aos seus usuários contas de e-mail institucionais com o domínio @prevduasbarras.rj.gov.br, que devem ser utilizadas exclusivamente para fins institucionais.

O uso do e-mail institucional é fundamental para garantir a autenticidade, a integridade, a confidencialidade e a rastreabilidade das comunicações oficiais, contribuindo para a proteção das informações, a padronização da comunicação, a preservação da imagem institucional e a mitigação de riscos relacionados a fraudes, vazamento de dados e uso indevido de informações.

As regras de acesso, envio, recebimento, armazenamento e utilização do correio eletrônico institucional devem observar rigorosamente as orientações desta Política de Segurança da Informação (PSI), as normas internas específicas, bem como as demais diretrizes estabelecidas pela Prefeitura Municipal de Duas Barras, sendo vedada a utilização de contas pessoais para o tratamento de assuntos oficiais do PREVDB.

6.9. ACESSO À INTERNET:

O acesso à rede mundial de computadores (internet), no ambiente de trabalho, deve ser regido por normas e procedimentos específicos, atendendo às determinações desta PSI, e demais orientações governamentais e legislação em vigor.

6.10. USO DAS REDES SOCIAIS:

A utilização de perfis institucionais mantidos em redes sociais com o objetivo de prestar atendimento e serviços públicos, divulgando ou compartilhando informações do PREVDB, deve ser regida por normas internas especificas e deve estar em consonância tanto com a PSI quanto com os objetivos estratégicos da instituição.

6.11. AQUISIÇÃO, DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS DE INFORMAÇÃO:

As atividades de aquisição, manutenção e desenvolvimento de sistemas de informação devem observar critérios e controles de segurança, com vistas a garantir o respeito aos atributos básicos de segurança da informação.

6.12. CONSCIENTIZAÇÃO, SENSIBILIZAÇÃO E CAPACITAÇÃO EM SIN:

O PREVDB deverá promover continuamente a capacitação, reciclagem e o aperfeiçoamento de todos os usuários da instituição, por meio de programas de divulgação, sensibilização, conscientização e capacitação em segurança da informação e comunicações, com o propósito de criar uma cultura de segurança dentro da instituição.

6.13. PLANO DE INVESTIMENTOS EM SIN:

Os investimentos em segurança da informação serão realizados de forma planejada e consolidados em um Plano de Investimentos em SIN e, no que couber, no Plano Diretor de Tecnologia da Informação (PDTIN).

O Plano de Investimentos em SIN deverá ser reavaliado quando houver revisão orçamentária ou revisão de prioridades das ações de SIN.

6.14. PROPRIEDADE INTELECTUAL:

As informações produzidas por usuários internos e colaboradores, no exercício de suas funções, são patrimônio intelectual do PREVDB e não cabe a seus criadores qualquer forma de direito autoral, ressalvado o direito de autoria, quando for o caso.

É vedada a utilização de patrimônio intelectual do PREVDB em quaisquer projetos ou atividades de uso diverso do estabelecido pela instituição, salvo autorização específica.

6.15. CONTRATOS, CONVÊNIOS, ACORDOS E INSTRUMENTOS CONGÊNERES:

Todos os contratos, convênios, acordos e instrumentos congêneres deverão conter cláusulas que estabeleçam a obrigatoriedade de observância desta PSI.

O contrato, convênio, acordo ou instrumento congênere deverá prever a obrigação da outra parte de divulgar esta Política, bem como suas normas complementares, aos empregados, prepostos e todos os envolvidos em atividades vinculadas ao PREVDB.

6.16. USO DE COMPUTAÇÃO EM NUVEM:

O uso de recursos de Computação em Nuvem, para suprir demandas de transferência e armazenamento de documentos, processamento de dados, aplicações, sistemas e demais tecnologias da informação, deve ser regido por normas específicas, atendendo a determinações desta PSI, e demais orientações governamentais e legislação em vigor, com vistas a garantir a disponibilidade, integridade, confidencialidade e autenticidade das informações armazenadas na nuvem, em especial aquelas sob custódia e gerenciamento de prestador de serviço.

6.17. USO DE DISPOSITIVOS MÓVEIS:

As diretrizes gerais de uso de dispositivos móveis para acesso às informações, sistemas, aplicações e e-mail do PREVDB devem considerar, prioritariamente, os requisitos legais e a estrutura da instituição, atendendo a esta Política de Segurança da Informação, e devem ser regidas por normas específicas, as quais contemplarão recomendações sobre o uso desses dispositivos.

6.18. USO DO PROCESSO ELETRÔNICO

O Instituto de Previdência dos Servidores Públicos do Município de Duas Barras – PREVDB adota um Sistema de Processos Eletrônicos contratado especificamente para a tramitação, controle e gestão de todos os processos administrativos da instituição.

Todos os processos internos e externos do PREVDB são instruídos, movimentados e arquivados exclusivamente por meio desse sistema eletrônico, o que garante maior eficiência administrativa, rastreabilidade das ações e conformidade com os princípios da transparência, economicidade, autenticidade e integridade das informações.

O Sistema de Processos Eletrônicos do PREVDB conta com mecanismos de segurança e controle de acesso, assegurando que apenas usuários devidamente autorizados possam visualizar ou editar documentos e processos sob sua responsabilidade.

Com o objetivo de garantir a disponibilidade e a continuidade dos serviços, o sistema dispõe de rotinas automáticas de backup (cópia de segurança), realizadas periodicamente, que permitem a recuperação das informações em caso de falhas, incidentes ou desastres, preservando a integridade e a confiabilidade dos dados institucionais.

O uso do processo eletrônico deve observar integralmente as orientações desta Política de Segurança da Informação (PSI), bem como as normas específicas emitidas pela gestão do PREVDB e pela Prefeitura Municipal de Duas Barras

7. PENALIDADES:

Ações que violem esta Política ou quaisquer de suas diretrizes, normas ou procedimentos, ou que infrinjam os controles de Segurança da Informação (SIN) serão devidamente apuradas, sendo aplicadas aos responsáveis as sanções penais, administrativas e civis cabíveis.

O usuário responderá disciplinarmente e/ou civilmente pelo prejuízo que vier a ocasionar à instituição, podendo culminar com o seu desligamento e, se aplicáveis, eventuais processos criminais.

8. COMPETÊNCIAS E RESPONSABILIDADES:

8.1. CONSELHO DE ADMINISTRAÇÃO

I. Aprovar a Política de Segurança da Informação do PREVDB.

8.2. DIRETORIA EXECUTIVA DO PREVDB

I. Dar suporte à promoção da cultura de segurança da informação e comunicações;

II. Aprovar a Política de Segurança da Informação (PSI);

III. Aprovar programa orçamentário específico para as ações de SIN, conforme proposto pelo Comitê de Segurança da Informação.

8.3. PRESIDÊNCIA DO PREVDB

I. Dar suporte à promoção da cultura de segurança da informação e comunicações;

II. Nomear o Gestor de Segurança da Informação;

III. Aplicar ações corretivas e disciplinares cabíveis nos casos de quebra de segurança.

8.4. GESTOR DE SEGURANÇA DA INFORMAÇÃO

I. Promover e disseminar a cultura de segurança da informação;

II. Coordenar a elaboração da Política de Segurança da Informação;

III. Coordenar as ações de segurança da informação;

IV. Acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança e submeter à Presidência do PREVDB, os resultados consolidados de tais investigações e avaliações;

V. Propor recursos necessários às ações de Segurança da Informação;

VI. Realizar e acompanhar estudos de novas tecnologias, quanto aos possíveis impactos na segurança da informação e comunicações;

VII. Propor normas e procedimentos relativos à Segurança da Informação;

VIII. Encaminhar os resultados consolidados dos trabalhos de auditoria de Gestão de Segurança da Informação à Superintendência do PREVDB;

IX. Prover os meios necessários para capacitação e aperfeiçoamento técnico dos membros da ETIR, bem como prover a infraestrutura necessária para o seu funcionamento;

X. Providenciar a divulgação interna desta PSI.

8.5. PROPRIETÁRIO DE ATIVOS DE INFORMAÇÃO

I. Descrever o ativo de informação;

II. Definir e gerir os requisitos de segurança para os ativos de informação sob sua responsabilidade em conformidade com esta PSI;

III. Garantir a segurança dos ativos de informação sob sua responsabilidade, por meio de monitoramento contínuo;

IV. Comunicar as exigências de SIN do ativo de informação a todos os custodiantes e usuários;

V. Conceder e revogar acessos aos ativos de informação;

VI. Comunicar à ETIR os riscos e a ocorrência de incidentes de SIN;

VII. Designar custodiante dos ativos de informação, quando aplicável.

8.6. CUSTODIANTE DOS ATIVOS DE INFORMAÇÃO

I. Proteger e manter os ativos de informação;

II. Controlar o acesso, conforme requisitos definidos pelo proprietário da informação e em conformidade com esta PSI;

III. Definir e gerir os requisitos de segurança para os ativos de informação sob sua responsabilidade em conformidade com esta PSI.

8.7. TERCEIROS E FORNECEDORES

I. Tomar conhecimento desta PSI;

II. Fornecer listas atualizadas de documentação dos ativos, licenças, acordos ou direitos relacionados aos ativos de informação objetos do contrato;

III. Fornecer toda a documentação dos sistemas, produtos e serviços relacionados às suas atividades.

8.8. USUÁRIOS

I. Conhecer e cumprir todos os princípios, diretrizes e responsabilidades desta PSI, bem como os demais normativos e resoluções relacionados à Segurança da Informação;

II. Obedecer aos requisitos de controle especificados pelos gestores e custodiantes da informação

III. Comunicar os incidentes que afetam à segurança dos ativos de informação à Ouvidoria.

9. DIVULGAÇÃO E CONCIENTIZAÇÃO:

A divulgação das regras e orientações de segurança da informação aplicadas aos usuários deve ser objeto de campanhas internas permanentes, disponibilização integral e contínua na Intranet, seminários de conscientização e quaisquer outros meios, com vistas à criação de uma cultura de segurança da informação no âmbito do PREVDB.

Cabe ao Gestor de Segurança da Informação providenciar a divulgação interna desta PSI e das normas dela decorrentes, inclusive com publicação na intranet do PREVDB, e desenvolver processo permanente de divulgação, sensibilização, conscientização e capacitação dos usuários sobre os cuidados e deveres relacionados à SIN.

10. ATUALIZAÇÃO E VALIDADE:

A SIN, digital ou física, é tema de permanente acompanhamento e aperfeiçoamento, devendo ser constantemente revista e atualizada, visando à melhoria contínua da qualidade dos processos internos.

Os instrumentos normativos gerados a partir desta PSI deverão ser revisados sempre que se fizer necessário, em função de alterações na legislação pertinente ou de diretrizes políticas do Governo Federal e/ou Municipal, conforme os seguintes critérios:

10.1. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (PSI)

I. Nível de Aprovação: Diretoria Executiva;
II. Periodicidade de Revisão: Anual, não podendo exceder 3 anos;

10.2. NORMAS DE SEGURANÇA DA INFORMAÇÃO

I. Nível de Aprovação: Gestor de Segurança da Informação (CGSIN);
II. Periodicidade de Revisão: Semestral;

10.3. PROCEDIMENTOS OPERACIONAIS

I. Nível de Aprovação: Área Técnica;
II. Periodicidade de Revisão: Semestral;

10.4. VALIDADE

Esta PSI tem prazo de validade indeterminado, portanto, sua vigência se estenderá até a edição de outro marco normativo que a atualize ou a revogue.

11. PRINCIPAIS SIGLAS:

ABNT - Associação Brasileira de Normas Técnicas GSI - Gestor de Segurança da Informação
GETIR - Gestão de Tratamento de Incidentes de Segurança em Rede Computacional
GESIN - Gestão de Segurança da Informação
GRSIN - Gestão de Riscos de Segurança da Informação IEC - International Electrotechnical Commission
ISO - International Organization for Standardization PSI - Política de Segurança da Informação
SIN - Segurança da Informação TI - Tecnologia da Informação
PDTIN - Plano Diretor de Tecnologia da Informação.

Duas Barras, 23 de janeiro de 2025.

_____
Yann Pinho da Cruz
Chefe do Departamento de Tecnologia da Informação