Título: **POLÍTICA DE SEGURANÇA INTEGRADA DA PRODEB**

RESUMO

Este documento estabelece as políticas e diretrizes de segurança integrada, no âmbito da PRODEB, assim como sua abrangência em relação às diversas áreas da empresa, nos seguintes aspectos:

- Segurança de pessoas, de bens patrimoniais e de meio ambiente;
- Segurança de redes de computadores;
- Segurança em sistemas, sites e aplicações web;
- Segurança da informação e proteção de dados.

SUMÁRIO

1 OBJETIVO

O objetivo desta política de segurança integrada é orientar as ações e procedimentos que promovam a continuidade do negócio da PRODEB, com confiabilidade e qualidade.

2 CONCEITUAÇÃO

- **Acordo de Confidencialidade** – Cláusula contratual ou instrumento específico que contém responsabilidades, direitos e deveres dos empregados, prestadores e prospectores de serviços, tais como leis de direitos autorais ou de proteção de dados, bem como a extensão da responsabilidade para fora das dependências da organização e após a rescisão do vínculo contratual.
- **Alta administração** – Conselho de Administração e Diretoria Colegiada da PRODEB.
- **Ambiente de Desenvolvimento** – Instalações de processamento de dados cuja plataforma tecnológica destina-se ao uso exclusivo dos técnicos desenvolvedores de sistemas e aplicativos.
- **Ambiente de Produção** – Instalações de processamento de dados cuja plataforma tecnológica destina-se ao armazenamento e execução dos sistemas e aplicativos.
- **Ambiente de Teste** – Instalações de processamento de dados cuja plataforma tecnológica destina-se a testes de execução dos sistemas e aplicativos, compreendendo, também, homologação.
- **Análise de Risco** – Processo pelo qual são relacionados os eventos, os impactos e avaliadas as probabilidades destes se tornarem reais.
- **Aplicativo ou programa** – Arquivo executável, autônomo, para realização de tarefa específica.
- **Arquivo de log** – Registro detalhado de todas as transações efetuadas durante a utilização de um aplicativo e necessário ao rastreamento do seu uso.
- **Ativo** – Patrimônio composto por bens e direitos da PRODEB.
- **Ativo Tecnológico** – Equipamentos ou programas de computador que suportam o ambiente organizacional e de negócios da PRODEB.
- **Componente de Rede** – Equipamento empregado na rede, incluindo sua infraestrutura, para comunicação, gerência e supervisão, incluindo hardware e software.
- **Computação em nuvem (Cloud Computing)** – Modalidade de computação na qual são utilizados recursos computacionais compartilhados e interligados através da internet e consumidos como serviço, pelos quais se paga pelo consumo efetivo.
- **Configuração** – Conjunto de características físicas e funcionais de hardware e software necessárias ao seu adequado funcionamento.
- **Conformidade** – Aderência a um padrão previamente estabelecido e aceito como ideal.
- **Dados Pessoais (LGPD)** – Toda informação relacionada a uma pessoa identificada ou identificável, portanto não se limita a nome, sobrenome, apelido, idade, endereço ou números de documentos, mas também pode incluir informações como endereço IP, dados de localização ou perfil de compras.
- **Dados Pessoais Sensíveis (LGPD)** – Dados relacionados às características e escolhas pessoais, tais como origem racial, opinião política, saúde, vida sexual, dado genético ou biométrico.
- **Dispositivos móveis** – Qualquer equipamento ou acessório portátil, capaz de se conectar à rede ou internet e processar e/ou armazenar dados, tais como: smartphone, smartwatch, tablet, notebook, netbook, PDA, coletores de dados e similares.
- **Encarregado (LGPD)** – Pessoa indicada pelo controlador, que atua como canal de comunicação entre o controlador, os titulares, o operador e a autoridade nacional.

- **LGPD** – Lei Geral de Proteção de Dados
- **Gestão de continuidade de negócios** – Processo abrangente de gestão que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio caso estas ameaças se concretizem, desenvolvendo a resiliência operacional necessária.
- **Gestão de segurança da informação** – Processo abrangente de gestão que desenvolve ações e métodos que visam a integração das atividades de gestão de riscos, gestão de continuidade do negócio, tratamento de incidentes, tratamento da informação, conformidade, credenciamento, segurança cibernética, segurança física, segurança lógica, segurança orgânica e segurança organizacional.
- **Mídia removível** – Dispositivo de que pode ser removido do respectivo aparelho de leitura permitindo transportar os dados, tais como pendrive, CD/DVD, HD externo, cartão de memória, etc.
- **Risco** – Resultado objetivo da combinação entre a probabilidade de ocorrência de um determinado evento e o impacto resultante.
- **Sistema** – Conjunto de programas que funcionam de forma integrada e consistente, com o objetivo de atender a uma necessidade específica, que pode ser voltada a negócios, tal como controle de estoque ou folha de pagamento ou técnica tal como o sistema operacional do computador ou dispositivo móvel.
- **Tratamento dos dados (LGPD)** – Toda operação que envolva algum tipo de manuseio de dados pessoais.
- **Usuário** – Qualquer colaborador, seja ele servidor, estagiário, cliente, parceiro, fornecedor, prestador de serviço, ou terceiro em geral que utiliza os recursos de tecnologia da informação disponibilizados pela PRODEB, mediante autorização para a execução de atividades ou exercício de direitos de acesso pré-estabelecidos de acordo com os instrumentos contratuais aplicáveis, em local ou jornada de trabalho.

3 DIRETRIZES

3.1. **Segurança Orientada ao Negócio** – As ações de segurança integrada serão sempre planejadas e aplicadas em função da avaliação dos riscos para o negócio da organização. A disponibilidade, uso, acesso e proteção das informações e recursos envolvidos, devem ocorrer sempre de forma a preservar a continuidade e a competitividade da PRODEB, em sua área de atuação.

3.2. **Abrangência e Divulgação** – A Política de Segurança Integrada da PRODEB abrange todos os seus colaboradores, independente do vínculo, e deve ser divulgada para toda a comunidade usuária, que deve ser formal e expressamente comunicada sobre suas responsabilidades.

3.3. **Avaliação de Riscos** – A avaliação de riscos na PRODEB deve ser periódica, devendo fazer parte do escopo os ativos tecnológicos, processos, ambientes e pessoas, estabelecendo os níveis atualizados e as ações corretivas necessárias.

3.4. **Propriedade da Informação** – Toda informação armazenada ou mantida pela PRODEB é considerada de propriedade da organização gestora dessa informação. A informação deve estar adequadamente protegida, qualquer que seja o meio de armazenamento, contra violação, alteração, destruição, acesso não autorizado e divulgação indevida. Os responsáveis por seu armazenamento, guarda e manuseio respondem por sua integridade, uso ou divulgação.

3.5. **Classificação da Informação** – Toda informação armazenada ou mantida pela PRODEB deve ser classificada quanto à sua confidencialidade, integridade e disponibilidade, obedecendo à legislação vigente. A recepção, guarda, disponibilização, circulação e descarte das informações, devem ser disciplinados por procedimentos, formalmente estabelecidos.

3.6. **Responsabilidade** – Cada colaborador que tenha acesso ou manipule informações armazenadas ou mantidas pela PRODEB é considerado responsável pela segurança dos ativos e informações que estejam sob sua custódia assim como por todos os atos executados sob sua chancela conforme identificações de acesso.

3.7. **Menor Privilégio** – O colaborador deve ter acesso apenas às informações, ativos e ambientes imprescindíveis ao pleno desenvolvimento do seu trabalho.

3.8. **Cláusulas Contratuais** – Todas as garantias necessárias ao cumprimento desta Política de Segurança Integrada devem ser estabelecidas contratualmente junto aos fornecedores e clientes. Os contratos devem prever os requisitos de segurança pertinentes, regras de conduta internas e externas, responsabilidades das partes durante a execução do contrato e as penalidades aplicáveis em caso de não cumprimento de cláusulas relativas à segurança da informação.

3.9. **Sigilo** – Todos os colaboradores da PRODEB devem assinar o Acordo de Confidencialidade. No caso dos prestadores de serviço, o sigilo deve ser também observado em cláusulas contratuais.

3.10. **Cultura de Segurança** – As pessoas contratadas pela PRODEB, a qualquer título, devem ser treinadas de forma contínua para o pleno exercício de suas funções, bem como sobre as políticas, normas e procedimentos de segurança.

3.11. **Continuidade dos Negócios** – Todos os elementos necessários para a plena continuidade do negócio devem ter sua operacionalidade garantida.

3.12. **Computação em Nuvem** – A contratação de serviço de computação em nuvem deve atender aos requisitos da Política de Segurança Integrada da PRODEB e às normas e legislação brasileiras, quanto à confidencialidade, propriedade e localização dos dados armazenados. A empresa contratada deve assegurar que segue os padrões das normas internacionais de segurança em nuvem, através de certificações emitidas por órgãos de segurança, reconhecidos internacionalmente.

3.13. **Ambiente Tecnológico** – O ambiente tecnológico deve ser mantido atualizado para atender aos níveis de segurança e de qualidade requeridos. A incorporação de novas tecnologias deve ocorrer sem o comprometimento dos níveis de segurança preestabelecidos.

3.14. **Dispositivos Móveis** – A política de uso de dispositivos móveis na empresa deve ser regulamentada através de normas e procedimentos de segurança específicos. Todo dispositivo móvel somente poderá ser utilizado para acessar à rede e/ou recursos computacionais, caso ofereça suporte para autenticação, no mínimo de usuário e senha. Normas e procedimentos adicionais devem ser elaborados para assegurar a gestão e monitoramento destes equipamentos.

3.15. **Conformidade com Requisitos Legais** – A gestão de segurança da informação deve atender aos requisitos legais dos órgãos regulatórios de segurança da informação do Governo Estadual e Federal, assim como, às normas ABNT de segurança de informação, aplicáveis ao negócio da empresa.

3.16. **Capacitação em Segurança da Informação** – A política de capacitação em segurança deve estabelecer Programas de conscientização e treinamento em Segurança da Informação de forma continuada.

3.17. **Proteção de Dados Pessoais** – Normas e procedimentos adicionais devem ser elaborados visando à proteção de dados pessoais em atendimento aos requisitos da legislação: Lei de Acesso Informação (LAI), Lei nº 12.527 de 18 de novembro de 2011 e Lei estadual nº12.618 de 28 de dezembro de 2012; Marco Civil da Internet, Lei nº 12.965, de 23 de abril de 2014; e da Lei Geral de Proteção de Dados (LGPD), nº 13.709, de 14 de agosto de 2018 e 13.853 de 9 de julho de 2019.

4 POLÍTICA DE SEGURANÇA DE PESSOAS, DE BENS PATRIMONIAIS E DE MEIO AMBIENTE

4.1 Quanto à Contratação e Gestão de Pessoas:

4.1.1. A contratação de colaboradores, a qualquer título, deve observar a legislação específica vigente e considerar referências de caráter pessoal, profissional e acadêmica;

4.1.2. Os gestores devem ser orientados a observar o comportamento e desempenho dos seus colaboradores, identificando problemas de ordem pessoal que possam comprometer a segurança da organização;

4.1.3. A contratação de colaboradores, a qualquer título, materiais, equipamentos e serviços, deve contemplar dispositivos que garantam o pleno cumprimento das políticas, normas e procedimentos de segurança em vigor na PRODEB, prevendo sanções no caso de descumprimento ou negligência na sua aplicação;

4.1.4. O colaborador à disposição de outro Órgão ou Instituição, em qualquer nível ou esfera de Governo, fica subordinado à política de segurança do órgão ou instituição ao qual está subordinado;

4.1.5. Quando do desligamento de colaboradores, devem ser revogados todos os seus dispositivos de acesso, físico e lógico, e o seu ingresso nas instalações da PRODEB deve obedecer aos mesmos critérios definidos para visitantes;

4.1.6. Devem ser definidos e divulgados entre os colaboradores medidas e procedimentos que minimizem o risco de acesso não autorizado, perda e danos às informações.

4.2 Quanto à Segurança Patrimonial:

4.2.1. O perímetro de segurança das instalações físicas da PRODEB deve ser definido e protegido de acessos não autorizados;

4.2.2. Os recursos de tecnologia da informação e comunicação devem estar abrigados em instalações apropriadas, sendo o seu acesso restrito a pessoas autorizadas;

4.2.3. Os ambientes físicos, internos e externos da PRODEB, devem ser classificados quanto ao grau de riscos e ameaças, com o intuito de disciplinar as ações de proteção;

4.2.4. Os projetos de construção e reforma devem atender a todos os requisitos de segurança vigentes;

4.2.5. A PRODEB deve possuir planos específicos que envolvam a plena conservação de suas instalações físicas e edificações;

4.2.6. A PRODEB deve possuir mecanismos securitários, para cobertura do seu patrimônio;

4.2.7. A infraestrutura e insumos necessários à continuidade do negócio devem ser protegidos e ter sua disponibilidade garantida.

4.3 Quanto ao Controle de Acesso Físico:

4.3.1. O acesso físico deve ser controlado e orientado, de maneira a disciplinar a movimentação e circulação de pessoas, materiais, equipamentos e veículos.

4.4 Quanto à Alienação Segura:

4.4.1. Na alienação ou reutilização de equipamentos ou dispositivos de armazenamento deve ser assegurada a remoção de todas as informações geradas durante seu uso, restabelecendo, sob o ponto de vista de armazenamento de informações, a condição original do equipamento ou dispositivo.

4.5 Quanto à Gestão Ambiental:

4.5.1. A preservação do meio ambiente natural, no tocante à conservação das áreas internas e circunvizinhas, deve ser garantida;

4.5.2. O descarte de materiais tóxicos ou poluentes deve ser formalmente disciplinado.

4.5.3. A prevenção da saúde do trabalhador deve ser implementada através da adoção de medidas sanitárias e procedimentos que proporcionem um ambiente seguro.

5 POLÍTICA DE SEGURANÇA DE REDES DE COMPUTADORES

5.1 Quanto aos Meios Lógicos e Físicos:

5.1.1. Todos os componentes de rede devem ser classificados de acordo com sua criticidade para a continuidade do negócio e preservados quanto às ameaças físicas e ambientais;

5.1.2. As informações que trafegam no ambiente de rede, devem ter garantidas a integridade e a confidencialidade, em conformidade com sua classificação;

5.1.3. Os ativos de rede só podem ser utilizados após a sua adequação aos padrões de segurança adotados pela PRODEB;

5.1.4. Os ativos de rede somente devem ser liberados para uso após a efetiva homologação, realizada em ambiente apropriado, distinto do ambiente de Produção, e devidamente documentada;

5.1.5. As intervenções no ambiente de rede só podem ser permitidas mediante autorização formal e competente supervisão;

5.1.6. As versões de software e configurações dos ativos de rede devem ser atualizadas de acordo com as recomendações do fabricante, recomendações da **Assessoria de Segurança da Informação e de Proteção de Dados - ASP,** e as melhores práticas de mercado.

5.2 Quanto à Monitoração:

5.2.1. O ambiente de rede deve ser monitorado, e esta ação deve ser obrigatoriamente documentada;

5.2.2. As responsabilidades quanto à execução e análise crítica da documentação gerada devem ser definidas.

5.3 Quanto à Documentação:

5.3.1. As documentações referentes à: topologia, descrição da rede, conexões externas, inventário e configuração dos ativos devem ser mantidas atualizadas e sempre preservando os registros históricos.

5.4 Quanto ao Controle de Acesso Lógico:

5.4.1. O acesso lógico à rede deve ser controlado de forma centralizada, através de procedimentos formais a partir do perfil de cada usuário, no qual estará definido seu nível de autorização;

5.4.2. Todo serviço de rede não autorizado deve ser bloqueado ou desabilitado;

5.4.3. Todas as transações em rede devem, obrigatoriamente, estar protegidas através de mecanismos de segurança;

5.4.4. A conta de acesso lógico deve ser de uso individual, permitindo a identificação e o rastreamento dos acessos do usuário, não sendo permitido o compartilhamento, reaproveitamento ou transferência de contas entre usuários, uso de contas genéricas ou de uso coletivo.

6 POLÍTICA DE SEGURANÇA EM SISTEMAS E APLICATIVOS

6.1 Quanto aos Aplicativos:

6.1.1. O gestor do aplicativo deve ser definido formalmente;

6.1.2. Para cada aplicativo deve ser desenvolvido um plano de segurança, incluindo ações de continuidade de operação, de acordo com sua criticidade;

6.1.3. A documentação das aplicações deve ser mantida atualizada;

6.1.4. Os acessos a aplicativos devem ser gerenciados objetivando controle de permissões e rastreamento, de acordo com as definições de perfis de usuários por funcionalidade;

6.1.5. Ambientes distintos devem ser definidos para desenvolvimento, homologação e produção de aplicativos, no mínimo;

6.1.6. Os produtos e versões só devem ser disponibilizados em Produção após homologação, comprovada através de documentação pertinente;

6.1.7. Os produtos e versões só devem ser disponibilizados em Produção após a verificação do cumprimento dos requisitos de segurança da informação, de acordo com as normas e diretrizes vigentes;

6.1.8. As versões de desenvolvimento e de produção devem ser controladas e armazenadas com suas respectivas configurações de ambiente tecnológico;

6.1.9. A PRODEB deve estabelecer mecanismos de proteção de direitos autorais sobre os aplicativos desenvolvidos por ela ou sob encomenda;

6.1.10. Os aplicativos devem ser desenvolvidos adotando ferramentas e metodologia padronizadas pela PRODEB, seguindo as normas e diretrizes de segurança da informação PRODEB aplicáveis ao desenvolvimento de sistemas e aplicativos;

6.1.11. Todos os registros de ocorrência, tais como arquivos de LOGs e notificações, previstos pelos perfis de acesso, devem ser obrigatoriamente mantidos de forma a permitir a plena recuperação de informações, para assegurar a rastreabilidade das transações e auditoria de segurança.

6.2 Quanto aos Sistemas Operacionais e Softwares Básicos

6.2.1. Todo o acervo de softwares e dados mantidos pela PRODEB em conformidade com seu perfil de utilização e especificidades deve ser passível de recuperação a partir de cópias de segurança;

6.2.2. A instalação de softwares no ambiente de Produção deve ser formalmente aprovada pela PRODEB, mediante a comprovação do licenciamento adequado para a finalidade, tipo de licença e quantidades específicas;

6.2.3. O ambiente operacional deve ser monitorado, registrando as ocorrências que sejam necessárias para: contabilização do uso de recursos, recuperação de informações em situações de falhas, auditorias e rastreamento de tentativas de violação;

7 POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E PROTEÇÃO DE DADOS

7.1 Quanto à Segurança da Informação e Proteção de Dados

7.1.1. Toda operação de tratamento de dados pessoais, em meios digitais ou não, deve ser documentada através de normas e procedimentos específicos sobre o tema e seguir a legislação vigente;

7.1.2. Todos os colaboradores deverão adotar boas práticas em riscos e segurança da informação, visando garantir prevenção à fraude e assegurar a integridade dos dados;

7.1.3. Os contratos da PRODEB junto a clientes e fornecedores devem ser adequados quanto à aderência à legislação de proteção de dados pessoais vigente, bem como às normas e procedimentos específicos sobre o tema.

7.2 Quanto ao Tratamento de Dados Pessoais

7.2.1. Deve ser estabelecido um processo formal de gestão do tratamento de dados pessoais na empresa, em conformidade com a legislação vigente;

7.2.2. Um representante legal deve ser indicado para atuar como Encarregado de Dados junto a Autoridade Nacional de Proteção de Dados;

7.2.3. Requisitos e medidas adicionais de segurança devem ser planejados para minimizar o risco de tratamento de dados pessoais;

7.2.4. O processo formal de gestão do tratamento de dados pessoais deve prever a realização cíclica de auditoria e análise crítica, em um processo de melhoria contínua;

7.2.5. Todos os contratos com colaboradores, clientes e fornecedores, devem prever as responsabilidades e atribuições das partes, assegurando o cumprimento da legislação de proteção de dados pessoais vigente.

7.2.6. Termos de Compromisso e Confidencialidade, Termos de uso, Termos de Consentimento e Códigos de Conduta e Integridade, devem ser adequados à legislação de proteção de dados pessoais vigente.

7.2.7. O processo de desenvolvimento de software deve incorporar em sua metodologia a avaliação dos requisitos adicionais de segurança, considerando o fluxo de dados pessoais em todas as fases do ciclo de vida do sistema.

7.2.8. Todos sistemas e aplicativos desenvolvidos pela PRODEB que tratem dados pessoais deverão conter o Termo de Uso e Privacidade disponibilizado em local de fácil acesso para conhecimento dos usuários.

8 RESPONSABILIDADES

8.1 Responsabilidades da Diretoria Colegiada:

8.1.1. Assegurar os recursos necessários à implementação da Política de Segurança Integrada;

8.1.2. Aprovar o Plano de Tratamento de Riscos;

8.1.3. Garantir o cumprimento da Política de Segurança Integrada definida neste documento;

8.1.4. Garantir a continuidade do negócio da PRODEB.

8.2 Responsabilidades do Comitê de Segurança Integrada e de Proteção de Dados

8.2.1. Promover e acompanhar as ações decorrentes da implementação e administração da Política de Segurança Integrada da PRODEB.

8.3 Responsabilidades da Assessoria de Segurança da Informação e de Proteção de Dados – ASP

8.3.1. Promover a elaboração de Planos de Ação específicos, objetivando a implementação da Política de Segurança Integrada da PRODEB, no tocante à segurança da informação e de proteção de dados;

8.3.2. Gerenciar o cumprimento da Política de Segurança Integrada da PRODEB, no tocante à segurança da informação e de proteção de dados;

8.3.3. Revisar periodicamente a Política de Segurança Integrada sugerindo ações que se façam necessárias;

8.3.4. Elaborar e executar Planos de Auditoria da Segurança da Informação com base na Política de Segurança Integrada da PRODEB;

8.3.5. Promover ações visando a conformidade da PRODEB com a sua Política de Segurança Integrada.

8.4 Responsabilidades das Gerências:

8.4.1. Implementar as ações de segurança definidas pela empresa;

8.4.2. Diligenciar junto aos colaboradores sob sua supervisão a compreensão e realização de ações que visem proteger os ativos da PRODEB.

8.5 Responsabilidades dos Colaboradores:

8.5.1. Cumprir a Política de Segurança Integrada da PRODEB;

8.5.2. Comunicar formalmente à Assessoria de **Segurança da Informação e de Proteção de Dados – ASP ou Gerência Financeira e Administrativa – GFA** qualquer irregularidade ou desvio de segurança, conforme o caso.

Alterações apreciadas e aprovadas pelo Conselho de Administração em Reunião Ordinária de 16.04.2021.