COMPANHIA DE PROCESSAMENTO DE DADOS DO ESTADO DE SÃO PAULO - PRODESP

Política de Segurança da Informação e Privacidade

Aprovado na reunião do Conselho de Administração em 24/fevereiro/2022

SUMÁRIO

Histórico das Revisões:

Rev. Nr.	Data	Descrição
00	24/02/2022	Aprovação pelo Conselho de Administração. Versão inicial (referência NP 25.00)
01	28/03/2022	Alteração Simples: atualização da capa com a data de aprovação pelo CA e alteração do sistema SGRCi para Sistema de Integridade Prodesp - SIP

1. INTRODUÇÃO

A Política de Segurança da Informação e Privacidade ("Política" ou simplesmente "PSI&P") é o documento que orienta e estabelece as diretrizes, procedimentos, mecanismos, competências, responsabilidades e valores a serem adotados para a Gestão de Segurança da Informação da PRODESP e tem como finalidade a proteção dos seus ativos de informação, dos dados pessoais, além da mitigação dos riscos de responsabilidade legal dos administradores e gestores da Empresa, bem como dos empregados e terceiros envolvidos.

Essa Política, de incumbência da área de Segurança da Informação, está orientada por cinco princípios:

- **Autenticidade:** É o pilar que valida a autorização do usuário para acessar, transmitir e receber determinadas informações. Seus mecanismos básicos são logins e senhas**,** mas também podem ser utilizados recursos como a autenticação biométrica, por exemplo. Esse pilar confirma a identidade dos usuários antes de liberar o acesso aos sistemas e recursos, garantindo que não se passem por terceiros;
- **Confidencialidade:** apenas pessoas devidamente autorizadas pela PRODESP devem ter acesso à informação;
- **Disponibilidade:** as informações devem estar disponíveis para as pessoas autorizadas sempre que necessário ou demandado;
- **Integridade:** apenas alterações, adições, supressões ou exclusões autorizadas pela PRODESP ou pelo titular do dado devem ser realizadas nas informações;
- **Privacidade:** É o direito à reserva de informações pessoais e da própria vida pessoal conforme determina a legislação vigente.

De modo a assegurar a observância dos referidos princípios e garantir a efetiva gestão da informação, essa Política, deve ser cumprida e aplicada em todas as áreas e unidades da empresa e ser de conhecimento de todos os empregados da PRODESP e suas Partes Relacionadas.

2. REFERÊNCIAS

A utilização das informações da PRODESP ou por ela custodiadas, bem como o tratamento de Dados Pessoais no ambiente da PRODESP e demais ambientes por ela controlados, devem estar de acordo com esta Política e outros documentos normativos oficiais da empresa, como o Código de Conduta e Integridade, disponíveis no site (http://www.prodesp.sp.gov.br/governanca-corporativa/regimentos-politicas.asp), e as Normas e Procedimentos disponíveis na intranet da empresa https://Intranetprodesp-governosp.msappproxy.net/intranet/verbete/normas-e-procedimentos-prodesp, estas de acesso restrito aos empregados e terceiros envolvidos, bem como com a legislação vigente.

Deverão ser observadas na aplicação desta Política a legislação e suas regulamentações aplicáveis, destacando-se:

- Lei federal n° 13.709/2018 – Lei Geral de Proteção de Dados Pessoais;
- Decreto estadual n° 65.347/2020 – Dispõe sobre a aplicação da Lei Geral de Proteção de Dados Pessoais, no âmbito do Estado de São Paulo;
- General Data Protection Regulation (EU GDPR) – Regulamento Geral de Proteção de Dados Europeu, conforme o caso;
- Lei federal n° 12.527/2011 – Lei de Acesso à Informação;
- Decreto estadual nº 58.052/2012 - Regulamenta a Lei federal n° 12.527, de 18 de novembro de 2011, que regula o acesso a informações, e dá providências correlatas
- Lei federal n° 9.279/1996 – Lei da Propriedade Industrial;
- Lei federal n° 12.965/2014 – Lei do Marco Civil da Internet;
- Código Penal Brasileiro;
- Lei federal nº 8.078/1990 - Código de Defesa do Consumidor.

A legislação pertinente, além de guias de boas práticas e normas, tais como a ABNT NBR ISO/IEC 27001, 27002 e 27701, estão listadas e sintetizadas no Catálogo Regulatório da PRODESP, de acesso exclusivo dos empregados da Empresa, disponível no Sistema de Integridade Prodesp - SIP.

3. OBJETIVO

Esta Política visa estabelecer as diretrizes exigidas para a proteção das informações e Dados Pessoais da PRODESP e por ela custodiados, de forma a garantir a Disponibilidade, Integridade, Confidencialidade, Autenticidade e Privacidade das informações e dos Dados Pessoais tratados durante o seu ciclo de vida.

Tem como objetivo orientar, por meio das definições estabelecidas pelas Normas e Procedimentos de Segurança da Informação que complementam esta PSI&P, os empregados e terceiros envolvidos que desempenham suas atribuições em regime presencial ou de teletrabalho, clientes que utilizam ativos de tecnologia da informação disponibilizados pela PRODESP, que eventualmente tenham acesso à dados controlados ou processados pela PRODESP.

Por fim, a PSI&P da PRODESP busca direcionar, apoiar e garantir que a empresa esteja em conformidade com as premissas do negócio, além de fornecer o devido respaldo para o exercício das atividades do Encarregado de Dados.

4. ABRANGÊNCIA

Esta Política abrange todos os sistemas, equipamentos e informações e dados da PRODESP ou por ela tratados, incluindo também seus empregados, independentemente do nível hierárquico, se permanentes ou comissionados, até mesmo os cedidos para outros órgãos/entidades, terceiros envolvidos e parceiros comerciais, que desempenham suas funções nas dependências da empresa – sede, filiais e unidades descentralizadas que operam com infraestrutura da PRODESP, em regime presencial e/ou de Teletrabalho.

5. DIRETRIZES GERAIS DA SEGURANÇA DA INFORMAÇÃO

A segurança e a proteção da informação e da privacidade dos dados pessoais são de responsabilidade de cada empregado da PRODESP em relação às informações que acessa, processa, monitora ou gerencia e aos dados pessoais que trata.

É obrigação de cada empregado e terceiros envolvidos manter-se atualizado em relação a PSI&P e aos procedimentos e normas relacionados, buscando orientação da Coordenadoria, Gerência ou Superintendência responsável pela condução da Segurança Corporativa, sempre que não estiver absolutamente seguro quanto à recepção, uso e/ou descarte de informações.

A responsabilidade pelo cumprimento desta PSI&P, em relação à segurança da informação e privacidade dos dados pessoais, deve ser comunicada na fase de contratação dos empregados e de prestadores de serviços. Todos os empregados ou terceiros envolvidos devem ser orientados sobre os procedimentos de segurança e privacidade, bem como sobre o uso correto dos ativos, informações e dados pessoais, a fim de mitigar possíveis riscos.

Os usuários dos sistemas desenvolvidos ou licenciados pela PRODESP devem utilizar as informações da PRODESP (dados corporativos) observando as determinações desta PSI&P e os dados pessoais de empregados ou de terceiros envolvidos em estrita obediência às referidas determinações, bem como às diretrizes contidas nas leis específicas e recomendações dos organismos de inspeção, como por exemplo, a Agência Nacional de Proteção de Dados - ANPD.

Situações de exceção e não previstas nesta PSI&P, deverão ser submetidas à análise e deliberação do Comitê de Segurança da Informação.

6. RESPONSABILIDADES

6.1. Empregados e terceiros envolvidos

As regras previstas nesta PSI&P devem ser observadas por todos os empregados e terceiros envolvidos da PRODESP, independentemente do emprego e natureza do vínculo com a empresa, com especial atenção para aquelas restritas a públicos específicos ou que exigem autorização especial.

Cada usuário deve acessar apenas as informações e os ambientes previamente autorizados. Qualquer tentativa de acesso a ambientes não autorizados será considerada uma violação desta PSI&P.

O acesso à informação e aos dados pessoais deve ser autorizado apenas para os usuários que deles necessitem para o desempenho das suas atividades profissionais.

Eventual identificação ou suspeita de venda ou promessa de venda de dados de clientes e de fornecedores e/ou informações corporativas, sob responsabilidade e de propriedade da Empresa, de que seja Controladora ou Operadora, para finalidades ilícitas, fraudulentas ou relativas à concorrência desleal, deverá ser objeto de apuração por meio de sindicância.

6.2. Empregados em Regime de Exceção (Temporários)

Os empregados em regime de exceção, tais como temporários e estagiários, devem entender os riscos associados à sua condição especial e cumprir rigorosamente o que foi previsto no respectivo contrato firmado com a PRODESP, além do previsto nesta Política e outras normas aplicáveis.

6.3. Gestores de Pessoas e/ou Processos

São atribuições dos Gestores de Pessoas e/ou Processos:

- Atribuir aos empregados, na fase de contratação e de formalização dos contratos individuais de trabalho, de prestação de serviços ou de parceria, a responsabilidade do cumprimento da PSI&P da PRODESP;
- Adaptar as normas, os processos, procedimentos e sistemas sob sua responsabilidade para atender a esta PSI&P;
- Providenciar o cadastro dos riscos e controles internos de segurança e privacidade de dados relacionados à Diretoria, Gerência ou processo sob sua responsabilidade, no sistema SIP da PRODESP;
- Esclarecer as dúvidas relacionadas à PSI&P dos seus liderados;
- Estimular a participação dos seus liderados em treinamentos designados pela Gerência de Recursos Humanos;
- Comunicar ao Encarregado de Dados os relatos que lhe foram feitos acerca do eventual uso de dado pessoal de forma contrária ao autorizado pelo Titular, sua transferência/ compartilhamento, cópia, venda, dentre outras ações contrárias a esta política e às leis de proteção de dados;
- Reportar ao superior imediato eventual identificação ou suspeita de venda ou promessa de venda de informação estratégica da PRODESP, ou dado pessoal de que seja Controladora ou Operadora, para concorrente da PRODESP, cabendo a ele registrar a ocorrência em fluxo documental correspondendo, visando a instauração de sindicância.

6.4. Custodiantes da Informação Corporativa e Dados Pessoais.

As áreas e profissionais que guardam e/ou que estejam incumbidas da proteção e vigilância da informação, ainda que transitoriamente, deverão mapear o fluxo dos dados e apontar os riscos relacionados, observando:

a) Dados Pessoais: as informações mapeadas e riscos identificados deverão ser apontados para o Encarregado de Dados;
b) Dados Corporativos: as informações mapeadas e riscos identificados deverão ser apontados para o núcleo de Riscos da PGC.

6.5. Áreas de Tecnologia da Informação

São responsabilidades das áreas de Tecnologia da Informação correlatas às: Diretoria de Desenvolvimento de Sistemas e superintendências a ela vinculadas: Superintendência de Clientes 1, Superintendência de Clientes 2, Superintendência de Governo Digital e Diretoria de Operações com suas gerências e superintendências: Superintendência de Operações do Data Center e Superintendência de Serviços de TI - em relação à segurança da informação:

- Testar a eficácia dos controles utilizados, informando aos gestores sobre os riscos residuais, providenciando quando pertinente, o seu devido cadastramento no sistema SIP;
- Acordar com os gestores o nível de serviço que será prestado e os procedimentos de resposta aos incidentes;
- Configurar os equipamentos, ferramentas e sistemas concedidos aos empregados com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos por esta PSI&P e documentos correlatos;
- Segregar as funções administrativas e operacionais a fim de restringir, ao mínimo necessário e/ou viável, os poderes de cada indivíduo e eliminar, ou ao menos reduzir, a possibilidade de um empregado ou terceiro envolvido excluir os logs e trilhas de auditoria das suas próprias ações;
- Gerar e manter as trilhas para auditoria com nível de detalhe suficiente para rastrear possíveis falhas e fraudes. Para as trilhas geradas e/ou mantidas em meio eletrônico, implantar controles de integridade para torná-las juridicamente válidas como evidências;
- Envidar os melhores esforços para garantir segurança especial aos sistemas com acesso público, fazendo guarda de evidências que permitam a rastreabilidade para fins de auditoria ou investigação;
- Administrar, proteger e testar as cópias de segurança dos programas e dados relacionados aos processos críticos e relevantes da PRODESP;
- Planejar, implantar, fornecer e monitorar a capacidade de armazenagem, processamento e transmissão necessários para garantir a segurança requerida pelas áreas de negócio;
- Atribuir cada conta ou dispositivo de acesso a computadores, sistemas, bases de dados e qualquer outro ativo de informação a um responsável identificável como pessoa física;
- Justificar eventual necessidade e autorização de criação de usuário (login) para terceiro, orientar o terceiro sobre as regras de uso dos dispositivos da PRODESP e monitorar o uso deles. A criação de usuário terceiro deverá estar atrelada à ordem de serviço e ser revalidada periodicamente (verificação da continuidade da necessidade de acesso ou da revisão do nível de acesso);

- Empenhar os melhores esforços para garantir, da forma mais rápida possível, mediante solicitação formal da área de Recursos Humanos, no caso de empregado, ou gestora do contrato, no caso de terceiros, o bloqueio de acesso de usuários por motivo de desligamento da empresa, movimentação entre áreas, incidente, investigação ou outra situação que exija medida restritiva para fins de salvaguardar os ativos e interesses da empresa;
- Proteger continuamente todos os ativos de informação da empresa contra código malicioso e fazer uso das melhores práticas de mercado de modo a permitir que todos os novos ativos, ferramentas de software, aplicativos ou sistemas só entrem para o ambiente de produção após estarem livres de código malicioso e/ou indesejado;
- Empregar os melhores esforços para garantir que não sejam introduzidas vulnerabilidades ou fragilidades no ambiente de produção da empresa em processos de mudança, sendo ideal a aplicação de práticas de trilha de auditoria de código e a proteção contratual, para controle e responsabilização no caso de uso de terceiros;
- Definir as regras formais para instalação de software e hardware em ambiente de produção corporativo, exigindo o seu cumprimento dentro da empresa;
- Manter comunicação efetiva com o Comitê de Segurança da Informação sobre assuntos relacionados ao tema que afetem ou tenham potencial para afetar a PRODESP;
- Realizar auditorias periódicas de configurações técnicas e análise de riscos;
- Responsabilizar-se pelo uso, manuseio, guarda de assinatura e certificados digitais;
- Envidar os melhores esforços para garantir que todos os servidores, estações e demais dispositivos com acesso à rede da empresa operem com o relógio sincronizado com os servidores de tempo oficiais do governo brasileiro (relógio atômico nacional);
- Implantar controles que gerem registros auditáveis para retirada e transporte de mídias das informações custodiadas pela TI, nos ambientes totalmente controlados;
- Monitorar o ambiente de TI, gerando indicadores e históricos, dentre outros, (i) de uso da capacidade instalada da rede e dos equipamentos, (ii) de tempo de resposta no acesso à internet e aos sistemas críticos da PRODESP, (iii) de períodos de indisponibilidade no acesso à internet e aos sistemas críticos da PRODESP, (iv) de incidentes de segurança (vírus, trojans, furtos, acessos indevidos, etc.), (v) relativos às atividades de todos os empregados durante os acessos às redes externas, inclusive internet (por exemplo: sites visitados, e-mails recebidos/enviados, upload/download de arquivos, entre outros);
- Garantir que, nas trocas internas de ativos de TI, as informações de um usuário, constantes em equipamento da empresa, sejam removidas de forma irrecuperável, antes da sua disponibilização a outro usuário;
- Quando determinado, subsidiar/ assistir as atividades investigativas, mantendo o sigilo de todas as atividades realizadas;

- Propor as metodologias e os processos específicos para a segurança da informação, como avaliação de risco e sistema de classificação da informação;
- Promover a conscientização dos empregados em relação à relevância da segurança da informação, pela realização de campanhas, palestras, treinamentos e outros meios de endomarketing e capacitação/ instrução;
- Apoiar a avaliação e a adequação de controles específicos de segurança da informação para novos sistemas ou serviços;
- Quando requerido, analisar criticamente incidentes em conjunto com o Comitê de Segurança da Informação;

As pessoas responsáveis pelos sistemas computacionais – empregados ou terceiros autorizados - podem, em decorrência da natureza de suas atividades e de seus privilégios como usuários, acessar os arquivos e dados de outros usuários. No entanto, esse acesso deve ocorrer, exclusivamente, no desempenho de atividades operacionais sob sua responsabilidade e nos limites necessários à sua realização. São exemplos de atividades operacionais: manutenção de computadores, realização de cópias de segurança, auditorias ou testes no ambiente.

6.6. Encarregado de Dados

Cabe ao Encarregado de Dados da PRODESP:

- Atender as demandas dos Titulares dos Dados dos quais a PRODESP é a Controladora e realizar atividades como, dentre outras: (i) recebimento e registro das solicitações, reclamações e comunicações dos Titulares, (ii) prestação de esclarecimentos e (iii) adoção de providências dentro dos prazos legais e definidos nas políticas da empresa, envolvendo, sempre que necessário, ao fiel e efetivo atendimento dos pedidos, outras áreas da empresa;
- Receber e registrar as comunicações da ANPD – Autoridade Nacional de Proteção de Dados, e de agências de proteção de dados internacionais, quando a PRODESP estiver abrangida por lei de aplicação extraterritorial, e adotar providências;
- Garantir que as reuniões presenciais ou online com representantes das agências de proteção de dados sejam realizadas sempre por, no mínimo, dois profissionais;
- Registrar em ata as reuniões realizadas com Agência Nacional de Proteção de Dados – ANPD;
- Observar as orientações do Código de Conduta e Integridade da PRODESP quanto à interação com agentes públicos, incluindo, mas não se limitando àqueles incumbidos das atividades de fiscalização;
- Orientar os empregados e os contratados a respeito das práticas a serem tomadas em relação à proteção de Dados Pessoais;
- Desempenhar suas atribuições em articulação com o Ouvidor Geral do Estado de São Paulo designado como Encarregado de Dados do Estado;

- Receber os registros de incidente de segurança da informação que contenham evidências de que o incidente diz respeito ou relaciona-se à proteção dos Dados Pessoais;
- Elaborar o RIPD - Relatório de Impacto à Proteção de Dados Pessoais e documentos equivalentes eventualmente exigidos por leis internacionais aplicáveis à PRODESP, envolvendo as áreas necessárias para apoio à composição do(s) documento(s), e transmiti-lo(s) à(s) respectiva(s) agência(s) solicitante(s), em atendimento à demanda formal;
- Receber e registrar as orientações das agências de proteção de dados e encaminhá-las às áreas que deverão tomar conhecimento;
- Executar as demais atribuições definidas pela Presidência ou normas complementares do Estado de São Paulo ou agências de proteção de dados;
- Contribuir com investigações, internas ou externas, relacionadas, dentre outras coisas, ao acesso não autorizado, uso inadvertido de dados pessoais;
- Contribuir com o mapeamento do ciclo de vida dos dados pessoais.

6.7. Comitê de Segurança da Informação

Cabe ao Comitê de Segurança da Informação (“CSI”), conforme definido em seu Regimento Interno:

- Analisar e validar a Política de Segurança Corporativa, Procedimentos e Normas sempre que necessário, a fim de garantir a Continuidade do Negócio da PRODESP;
- Validar as análises de riscos e impactos de Segurança da Informação, nos âmbitos: estratégico, tático e técnico;
- Se reunir periodicamente para tratar de assuntos de Segurança da Informação;
- Discutir propostas de investimentos estratégicos relacionados à segurança da informação e proteção da privacidade dos Dados Pessoais com o objetivo de reduzir riscos;
- Avaliar os incidentes de segurança e propor ações corretivas de âmbito corporativo estratégico;
- Registrar no Canal de Denúncias da PRODESP a suspeita ou o conhecimento de atuação deliberada de infração a essa Política, ao Código de Conduta e Integridade da PRODESP, leis de proteção de dados, de propriedade intelectual e anticorrupção, dentre outras leis aplicáveis aos negócios da empresa;
- Definir as medidas cabíveis nos casos de descumprimento da PSI&P e/ou das Normas de Segurança da Informação complementares;
- Observar o Ciclo de PDCA corporativo através de indicadores, realizando aprovações e propondo ajustes quando necessários de forma a permitir a evolução contínua nos processos que estejam relacionados à Segurança da Informação.

6.8. Gerência de Conformidade, Gestão de Riscos e de Controle Interno - PGC

São atribuições da Gerência, no âmbito desta Política:

- Orientar as áreas quanto à identificação e classificação dos riscos, e apontamento dos controles internos necessários à sua mitigação e gestão;
- Prestar apoio, quando solicitado, ao Encarregado de Dados em assuntos específicos, sem qualquer prejuízo à independência da PGC ou do Encarregado;
- Apoiar os treinamentos relativos a essa Política, o que inclui, mas não se limita (i) à análise do conteúdo dos treinamentos, (ii) definição dos públicos-alvo, (iii) condução dos treinamentos e ministração de palestras;
- Atualizar o Código de Conduta e Integridade da PRODESP e demais políticas sob sua responsabilidade, para que reflitam as leis e boas práticas de segurança da informação;
- Acompanhar a interação do Encarregado de Dados com a ANPD;
- Verificar a conformidade dos processos e procedimentos de segurança da informação, de modo a garantir a observância das leis aplicáveis e políticas internas;
- Garantir a confidencialidade dos dados pessoais a que tiver acesso em atividades de apuração de fatos oriundos do Canal de Denúncias;
- Monitorar os riscos mapeados pelas áreas, identificados como estratégicos;
- Participar do Comitê de Segurança.

6.9. Áreas de Desenvolvimento de Software

Compete às áreas de desenvolvimento de software:

- Garantir que os requisitos de segurança da informação estejam implementados nos sistemas desenvolvidos e que sejam mantidos à luz das melhores práticas de desenvolvimento seguro (em inglês denominado, “SSDF” ou “Secure Software Development Framework”);
- Garantir a transparência do Tratamento de Dados realizados para os Titulares ou para atendimento das políticas da empresa, conforme diretivas das leis de proteção de dados;
- Não realizar nenhum tratamento de Dados Pessoais em ambientes de desenvolvimento ou homologação, conforme Norma de Acesso e Disponibilidade de Dados e procedimento conexo;
- Criar, mediante auxílio do Encarregado de Dados, da PGC e da área jurídica, os termos e condições gerais de uso dos softwares desenvolvidos, bem como outros documentos pertinentes;
- Envidar os melhores esforços para garantir que os bancos que contenham Dados Pessoais estejam em formato interoperável e estruturado, conforme estabelece a LGPD, de maneira a permitir o uso compartilhado da informação, com vistas à

execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral;

- Permitir através do desenvolvimento de software, que sejam inseridas técnicas para verificação de trilha de auditoria dos usuários dos sistemas que tratarem dados, sensíveis, confidenciais e financeiros de forma a identificar, em caso de necessidade, os responsáveis pelos acessos;
- Proteger o patrimônio intelectual da PRODESP, particularmente quanto aos softwares desenvolvidos, desenhos de software, regras de negócio, documentações e artefatos produzidos, mantendo sua guarda em repositórios institucionais definidos pela empresa.

6.10. Recursos Humanos

A Gerência de Recursos Humanos deve exigir dos empregados a assinatura do Termo de Responsabilidade, que dispõe sobre o cumprimento e observância das normas estabelecidas nesta Política e procedimentos correlatos, bem como de manter sigilo e confidencialidade das informações colocadas à sua disposição ou identificadas como resultado da prestação de serviços à PRODESP ou quaisquer de seus clientes e/ou parceiros, mesmo quando findo o vínculo laboral ou comercial com a PRODESP.

Compete também à Gerência de Recursos Humanos comunicar sobre a necessidade de criação de novo usuário, suspensão ou exclusão de acesso, às áreas responsáveis pela criação de usuários (logins) nos sistemas proprietários ou de terceiros.

6.11. Auditoria Interna

A Auditoria Interna deve providenciar rotinas regulares de auditorias para certificar os níveis adequados de Segurança da Informação e Privacidade, visando a adequada proteção da informação corporativa e dos Dados Pessoais tratados pela PRODESP.

É também de responsabilidade da auditoria interna:

- Subsidiar as auditorias externas das informações necessárias/ solicitadas;
- Nos casos de incidente de segurança da informação, conduzir auditoria investigativa.

6.12. Área Jurídica

Compete à área jurídica, dentre outras coisas:

- Observar a adoção de medidas de segurança da informação para a proteção dos dados pessoais constantes em contratos, termos, acordos, procurações e outros documentos legais que receba ou produza, a fim de preservar as diretrizes desta PSI&P;

- Informar à Comissão de Avaliação de Documentos e Acesso - CADA acerca das orientações recebidas dos Controladores de Dados, naquilo que for pertinente aos dados compartilhados/ transferidos para a área jurídica;
- Orientar, sempre que necessário, o Encarregado de Dados na resposta às demandas das agências de proteção de dados;
- Assistir as áreas de tecnologia da informação na análise de políticas e termos de uso das tecnologias licenciadas pela PRODESP, quando envolver matérias relacionadas à presente PSI&P;
- Observar a atualização das minutas de contratos, termos, acordos e outros documentos legais recebidos, atentando-se para a evolução normativa das matérias relacionadas a esta Política, sugerindo adequações e fornecendo as orientações necessárias à área demandante;
- Observar a existência da cláusula de confidencialidade ou como anexo Acordo de Confidencialidade em todos os contratos recebidos, como condição imprescindível para que possa ser concedido o acesso aos ativos de informação disponibilizados pela PRODESP, sugerindo adequações e fornecendo as orientações necessárias à área demandante;
- Orientar juridicamente o Encarregado de Dados, sempre que necessário, sobre a aplicação da LGPD nos tratamentos de dados realizados pela empresa, como por exemplo, na identificação dos papéis de Operador e Controlador e na indicação da hipótese legal que permite o tratamento;
- Incluir no sistema SIP os riscos relativos a dados pessoais relacionados à área jurídica e apontar os controles internos implementados, quando pertinente;
- Prestar assessoria jurídica às áreas de negócio da PRODESP acerca das leis de proteção de dados, o que inclui, mas não se limita a: (i) orientar sobre a confirmação do papel da PRODESP, se Controladora ou Operadora, em função do objeto de contratações, (ii) questões que envolvam prazo de temporalidade de guarda de documentos e aspectos relacionados a outras leis, (iii) questões envolvendo situações de compartilhamento e comercialização de dados, (iv) questionamentos e dúvidas em aspectos e particularidades de execução de políticas públicas que envolvam matéria tratada na presente PSI&P.

6.13. Reponsabilidades da Comissão de Avaliação e Documentos e Acesso - CADA

Compete à Comissão de Avaliação de Documentos e Acesso - CADA, no âmbito desta PSI&P:

Quanto à gestão documental:

- atuar como agente multiplicador das normas e procedimentos da gestão documental, observando a proteção de dados pessoais e das informações corporativas nos termos da legislação vigente e dessa PSI&P;

- orientar a aplicação dos Planos de Classificação e das Tabelas de Temporalidade de Documentos em consonância com a legislação de proteção de dados pessoais e outras pertinentes a essa PSI&P, realizando as adequações eventualmente necessárias;
- orientar os procedimentos para eliminação, transferência ou recolhimento de documentos em conformidade com as diretrizes desta PSI&P e contexto legal da proteção de dados pessoais e das informações corporativas;

Quanto ao acesso:

- manifestar-se sobre os prazos mínimos de restrição de acesso aos documentos, dados ou informações pessoais para a correta aplicação desta PSI&P;
- propor a renovação, alteração de prazos, reclassificação ou desclassificação de dados e informações públicas, sigilosas e pessoais, assim como os procedimentos para a proteção destes, sempre que necessário, e, em consonância com a legislação vigente, visando a aplicação adequada desta PSI&P;
- orientar sobre a correta aplicação dos critérios de restrição de acesso constantes das tabelas de documentos, dados e informações sigilosas e pessoais;
- manifestar-se sobre os prazos mínimos de restrição de acesso aos documentos, dados ou informações pessoais, quando provocada e em eventuais dúvidas na aplicação efetiva desta PSI&P.

7. DA UTILIZAÇÃO

7.1 De Dados Corporativos

Todo dado corporativo e informação produzida ou recebida pelos (i) empregados da PRODESP, como resultado da atividade laboral, (ii) parceiros comerciais, como fruto da prestação de serviços, apresentação ou venda de produtos, termo ou acordo firmado com a PRODESP, (iii) donatários, em decorrência de Contrato de Doação, (iv) patrocinados, devido a Contrato de Patrocínio, (v) conveniados em razão de Convênio, e (vi) outros terceiros que venham a acessar dado corporativo, pertence à PRODESP, a não ser que expressamente esteja definido em contrário.

A alteração, tratamento ou exclusão de referidos dados está condicionada à autorização prévia e expressa da PRODESP e, via de regra, atrelados ao contrato, termo ou acordo firmado com a empresa.

A conclusão da relação laboral, comercial ou de parceria com a PRODESP obriga a contraparte de posse dos Dados Corporativos da PRODESP a devolvê-los ou destruí-los, conforme orientação da PRODESP.

7.2 De Dados Pessoais

Todo dado pessoal pertence ao seu Titular e só pode receber o Tratamento conforme acordado formalmente com o Controlador responsável ou autorização expressa do Titular.

O tratamento de tais dados deve ser registrado conforme estabelece a Norma NP-025 - “Norma de Acesso e Disponibilidade de Dados” visando a sua rastreabilidade, considerando que os Titulares de Dados e os órgãos de controle, como a ANPD, poderão solicitá-los a qualquer momento. Estes registros devem estar seguros e protegidos.

7.3 Da Informação e Recursos

As informações e os recursos de informática são disponibilizados única e exclusivamente àqueles que necessitem deles para o exercício de suas funções e apenas após terem concordado com o conteúdo do Termo de Responsabilidade e do Termo de Uso e Guarda de Equipamento, descrito em procedimento específico, e o assinado.

A liberação do acesso à informação para os empregados será autorizada pelo gestor que considerará a necessidade de acesso, os riscos envolvidos e o sigilo da informação para a realização dos objetivos da PRODESP. A liberação de acesso aos dados pessoais só poderá ser permitida desde que não viole os tratamentos permitidos, acordados oficialmente com o Controlador e de maneira que não coloque em risco de segurança dos dados.

Cada empregado deve acessar apenas as informações e os ambientes, físicos e virtuais, previamente autorizados. Qualquer tentativa de acesso consciente a ambientes não autorizados será considerada uma violação desta PSI&P. Tentativa de acessos não autorizados intencionais a Dados Corporativos ou Pessoais podem resultar na aplicação de medidas trabalhistas e/ou legais contra o infrator.

Os acessos às informações e aos dados pessoais devem ser registrados, de modo que a qualquer momento estejam disponíveis as informações sobre tentativas, frustradas ou não, de acesso às informações e dados (garantia da rastreabilidade).

O acesso aos sistemas – proprietários e licenciados – e diretórios da PRODESP e, consequentemente, às informações neles armazenadas, ocorre por meio da identificação e autenticação do usuário (login e senha), que são pessoais e intransferíveis, conforme estabelece a Norma NP-008 - “Controle de Acesso Lógico”.

Referidos dados para a autenticação do usuário devem ser mantidos em sigilo e possuir o mais alto nível de classificação da informação. As senhas deverão ser substituídas periodicamente, voluntariamente ou em atendimento aos Termos e Condições de Uso de cada software.

7.4 Dos Computadores e Recursos Tecnológicos

Os equipamentos tecnológicos (computadores desktop, laptops, celulares, dentre outros) disponibilizados aos empregados são de propriedade da PRODESP ou por esta alugados, cabendo ao usuário (também denominado cessionário) utilizá-los e manuseá-los corretamente e para o atendimento dos interesses da empresa, bem como cumprir as recomendações constantes nos procedimentos operacionais fornecidos pelas gerências responsáveis.

É proibido todo procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação, que devem ser realizados pela equipe da Gerência de Outsourcing de TI, conforme chamado técnico no Service Desk.

Todas as atualizações e correções de segurança do sistema operacional ou aplicativos somente poderão ser feitas após a devida validação no respectivo ambiente de homologação, e depois de sua disponibilização pelo fabricante ou fornecedor.

Os sistemas e computadores devem ter versões do software antivírus instaladas, ativadas e atualizadas permanentemente. O usuário, em caso de suspeita de vírus ou problemas na funcionalidade, deverá acionar a área técnica responsável mediante registro de chamado no Service Desk.

Os usuários deverão se abster de gravar arquivos nos computadores, por exemplo, no drive “C:”, que, se identificados, poderão ser excluídos instantaneamente e sem aviso prévio. Os arquivos recebidos ou produzidos no desempenho das funções na PRODESP deverão ser salvos em drives de rede.

Em caso de perda, furto ou roubo de equipamento fornecido pela PRODESP, o empregado deverá proceder conforme Norma de Utilização dos Equipamentos de Telefonia Móvel e, havendo suspeita ou conhecimento de que o dispositivo armazenava dados pessoais, o Encarregado de Dados da PRODESP deve ser informado imediatamente conforme estabelecido no “Fluxo Documental – Incidentes de Segurança – LGPD”.

O empregado será o único responsável por quaisquer danos, diretos ou indiretos, presentes ou futuros, que venha causar à PRODESP e/ou a terceiros pelo uso indevido dos equipamentos colocados à disposição pela empresa.

7.5 De Recursos Eletrônicos Pessoais

As informações estruturadas e sistemas da PRODESP somente serão utilizados em recursos da PRODESP, a não ser que expressamente autorizado pelo gerente da área, conforme procedimento previsto em norma específica.

O armazenamento de dados pessoais, sensíveis ou de menores de clientes (Controladores) não é permitido em equipamentos pessoais e Dispositivos Móveis.

7.6 Do e-mail Corporativo

As contas de e-mail disponibilizadas pela PRODESP são de propriedade da PRODESP e seu uso deve observar as políticas internas, as leis, a moral e os bons costumes.

O usuário de e-mail corporativo deve:

- Comprometer-se a escrever e-mails em linguagem profissional e de maneira que não comprometa a imagem da PRODESP, não viole a legislação vigente e nem os princípios éticos da empresa;
- Estar ciente de que (i) é o único e exclusivo responsável pelo uso da conta de e-mail criada e colocada à disposição pela PRODESP, para o desempenho de atividades laborativas; (ii) a criação de e-mail utilizando o nome e sobrenome do usuário objetiva exclusivamente sua identificação, não configurando seu uso infração às leis de proteção de dados, tampouco a transferência da titularidade da conta de e-mail; (iii) o conteúdo do e-mail ou correio eletrônico corporativo de cada usuário pode ser acessado e monitorado pela PRODESP sempre que for necessário, devendo os empregados ter ciência de que tais acessos e monitoramentos visando a segurança e proteção dos dados, podem ser feitos sem aviso prévio aos usuários.

As mensagens de correio eletrônico sempre deverão incluir assinatura com o seguinte formato:

- Nome do empregado
- Gerência ou departamento
- Nome da empresa
- Telefone(s)
- Correio eletrônico ou endereço do e-mail

7.7 Dos Programas de Computador

Todo e qualquer programa de computador utilizado deve ser de propriedade da PRODESP, ou estar devidamente licenciado pelo desenvolvedor e homologado pela PRODESP.

O uso de software não pago (gratuito, open source, GPL, GNU e semelhantes) só será permitido após homologação e autorização formal da Coordenadoria de Segurança de Rede do Data Center – CSRD.

7.8 Do Ambiente de Internet

O uso do ambiente de internet da PRODESP, por meio de equipamento cedido pela empresa, pessoal ou de terceiros, está sujeito a monitoramento pela PRODESP, que se reserva ao direito de, a qualquer momento e sem aviso prévio, bloquear qualquer arquivo, site, correio eletrônico, domínio ou aplicação armazenados na rede/internet – esses bloqueios, quando o usuário da rede/ internet for empregado da empresa, poderão ser realizados em disco local, na estação trabalho ou em áreas privadas da rede.

No uso da internet da PRODESP, não é permitido:

- a alteração de configuração ou parâmetro de segurança, atividade restrita às equipes de suporte;
- a divulgação e/ou o compartilhamento indevido de informações da área administrativa em listas de discussão, sites ou comunidades de relacionamento, salas de bate-papo ou chat, comunicadores instantâneos ou qualquer outra tecnologia correlata que venha surgir na internet;
- utilizar os recursos da PRODESP para fazer o download ou distribuição de software ou dados pirateados, atividade considerada delituosa de acordo com a legislação nacional;
- o acesso, exposição, armazenamento, distribuição, gravação, transferência ou qualquer ato que contrarie a moral ou os bons costumes, de material de cunho sexual;
- o upload (subida) de qualquer software licenciado da PRODESP, ou de dados de sua propriedade, aos parceiros, clientes e quaisquer terceiros, a não ser que excepcionalmente e expressamente autorizado pela Diretoria Executiva;
- utilizar os recursos da PRODESP para, deliberadamente, propagar qualquer tipo de vírus, worm, cavalo de troia, spam, mensagens com discurso de ódio, discriminatórias, religiosas, políticas, de ordem pessoal (particular) ou de assédio, ou programas de controle de outros computadores; e
- o acesso a softwares peer-to-peer (Kazaa, BitTorrent e afins).

A internet disponibilizada pela empresa aos seus empregados em trabalho presencial, independentemente da natureza da relação contratual, pode ser utilizada para fins pessoais, desde que não prejudique o andamento dos trabalhos, não comprometa a banda da rede e observe as normas internas e legislação vigente, como a NP-023 Acesso à Internet que define a forma de uso para os empregados.

Os serviços de streaming (rádios on-line, canais de broadcast e afins) serão permitidos a grupos específicos, devidamente autorizados pelas Superintendências demandantes.

8. PROTEÇÃO DA INFORMAÇÃO E DA PRIVACIDADE DE DADOS

8.1 Orientações Gerais

Toda informação da PRODESP (Dados Corporativos) e custodiada por ela, incluindo dados pessoais, devem ser protegidos para que não sejam alterados, acessados, destruídos ou sejam objeto de qualquer outro tipo de operação ou tratamento indevido ou não autorizado.

A manipulação, divulgação, violação da privacidade da informação ou uso indevido, no todo ou em parte, de informações por parte de qualquer pessoa ou empresa é considerada falta e implicará, no caso de empregado, na aplicação de sanções disciplinares, trabalhistas e legais; no caso de parceiro comercial, na rescisão do contrato, incidência das penalidades eventualmente previstas, além das medidas legais cabíveis.

O envio de cópia, total ou parcial, de base de dados ou cópia de arquivos que não estejam previamente autorizados em contrato ou especificação técnica, para ambientes externos ao Data Center da PRODESP ou para ambientes diferentes do ambiente de produção, devem ser formalmente autorizados pelo cliente proprietário da informação conforme Norma NP-025 - "Norma de Acesso e Disponibilidade de Dados", sendo este solidário por eventuais incidentes de segurança quanto à confidencialidade, utilização, disponibilidade, privacidade e integridade destas informações, salvo apuração em sentido contrário.

O acesso aos locais ou edifícios é restrito ao pessoal autorizado. Os locais onde se encontram os recursos de informação contam com proteção e controle de acesso físico e são monitorados por câmeras. As informações dos transeuntes, bem como dos profissionais que trabalham nesses locais, e suas imagens são tratadas como dados pessoais, sendo seu uso restrito ao cumprimento desta PSI&P, Código de Conduta e Integridade da PRODESP e respectivo contrato firmado com a empresa.

O trânsito de visitantes na empresa está condicionado ao acompanhamento por um empregado da PRODESP, sendo a entrada e permanência em locais ou edifícios de acesso restrito.

Os visitantes só podem acessar as redes locais da PRODESP (redes específicas para visitantes) sejam cabeadas ou wi-fi (Rede Local), após devida autorização da área responsável e devem ser acompanhados pelo responsável pela visita.

O uso de crachá de identificação, em local visível e com a identificação virada para frente, é obrigatório em todas as dependências da PRODESP, pelos empregados e visitantes.

É obrigação de todo empregado comunicar ao pessoal de segurança física sobre visitante não acompanhado ou qualquer pessoa que não esteja usando uma identificação visível (crachá).

Deverão ser criados e instituídos controles apropriados, trilhas de auditoria ou registros de atividades, em todos os pontos e sistemas em que a empresa julgar necessário para reduzir os riscos dos seus ativos de informação e de dados pessoais, como, por exemplo, nas estações de trabalho, notebooks, nos acessos à internet, no e-mail ou correio eletrônico, nos sistemas comerciais e financeiros desenvolvidos ou em uso pela PRODESP ou por terceiros.

Os ambientes de produção devem ser segregados e rigidamente controlados, garantindo o isolamento necessário em relação aos ambientes de desenvolvimento, testes e homologação.

8.2 Identificação

Os dispositivos de identificação e senhas protegem a identidade do empregado-usuário, evitando e prevenindo que outra pessoa se faça passar por ele perante a PRODESP e/ou terceiros[1].

[1] O uso dos dispositivos e/ou senhas de identificação de outra pessoa constitui crime tipificado no Código Penal Brasileiro (art. 307 – falsa identidade).

Todos os dispositivos de identificação utilizados na PRODESP, como o número de matrícula do empregado, crachá, as identificações de acesso aos sistemas, certificados, assinaturas digitais, dados biométricos ou qualquer outro meio que venha a ser adotado pela empresa ou decorra de lei, têm de estar associados a uma pessoa física e atrelados inequivocamente aos seus documentos oficiais reconhecidos pela legislação brasileira.

A Gerência de Recursos Humanos da PRODESP é o responsável pela emissão e pelo controle dos documentos físicos de identidade dos empregados, enquanto a Gerência de Outsourcing de TI responde pela criação da identidade lógica dos empregados na empresa, nos termos do Procedimento para Gerenciamento de Contas de Grupos e Usuários.

O usuário, vinculado aos dispositivos identificadores lógicos, será responsável pelo seu correto uso perante a empresa e terceiros relacionados, devendo, portanto:

a) abster-se de:

a.1) compartilhá-los com outras pessoas;

a.2) compartilhar login para funções de administração de sistemas;

a.3) anotar ou armazenar as senhas em arquivos eletrônicos (Word, Excel, etc.), compreensíveis por linguagem humana (não criptografados);

a.4) criar senhas baseadas em informações pessoais, como próprio nome, nome de familiares, data de nascimento, endereço, placa de veículo, nome da empresa, nome do departamento;

a.5) criar senhas constituídas de combinações óbvias de teclado, como “abcdefgh”, “87654321”, entre outras.

b) e comprometer-se a:

b.1) trocar imediatamente a senha, adotando a prática de estabelecer senhas “Fortes” (utilizar letras maiúsculas, minúsculas, números e caracteres especiais) conforme as orientações apresentadas, após realizar o primeiro acesso ao ambiente de rede local;

b.2) memorizar a própria senha, bem como a proteger e guardar dos dispositivos de identificação que lhe forem designados.

Se existir login de uso compartilhado por mais de um empregado, a responsabilidade perante a PRODESP e a legislação (cível e criminal) será dos usuários que dele se utilizarem.

Todos os acessos aos ambientes físicos e virtuais da PRODESP devem ser imediatamente bloqueados com o fim da relação comercial ou laboral do usuário com a empresa. As solicitações de bloqueios serão feitas pela Gerência de Recursos Humanos via ITSM. No caso de terceiros, o Coordenador da área onde o terceiro presta serviço, deverá solicitar os bloqueios imediatamente ao desligamento.

8.3 Teletrabalho

As informações estruturadas e os sistemas da PRODESP somente deverão ser utilizados em recursos da PRODESP, por meio de acesso oficial disponibilizado aos usuários, para prevenir o processamento e o armazenamento da informação em um equipamento de propriedade particular.

Não é permitido o armazenamento de dados pessoais ou informações estruturadas, arquivos, códigos ou dados que pertençam à PRODESP em disco rígido de equipamento de uso pessoal (ex: pendrive, HD externo, notebook, tablet, entre outros). Estes arquivos devem sempre ser armazenados dentro da rede corporativa da PRODESP.

Os equipamentos utilizados para teletrabalho que são de propriedade da PRODESP deverão ser utilizados exclusivamente por empregados, sendo a guarda e uso correto conforme estabelecido nesta política de única responsabilidade do usuário.

A propriedade intelectual da PRODESP deve ser preservada pela estrita observância das políticas, documentos ou procedimentos relativos a direitos autorais e à propriedade intelectual, para evitar disputas relativas à matéria em decorrência de criações/ desenvolvimento em equipamentos particulares.

Quando aplicável, efetuar a devolução do equipamento da PRODESP utilizado nas atividades de trabalho remoto.

8.4 Software em Demonstração/Teste

Todo software a ser instalado na PRODESP para (i) demonstração, com o objetivo de conhecimento da sua finalidade, conteúdo, abrangência, funcionalidades, facilidades e, principalmente, de sua real aplicabilidade às necessidades da empresa, ou (ii) teste, com a finalidade de verificar se seu desempenho satisfaz às exigências e demandas de um determinado projeto ou ambiente da PRODESP, deve ser instalado conforme diretrizes previstas na Norma 25.26 de Software em Demonstração/Teste.

8.5 Data Center

O acesso ao Data Center deve ser observado conforme perfil dos empregados que executam atividades no ambiente do mesmo e controlado por sistema de autenticação que observe os mais rigorosos critérios de segurança, por exemplo: biometria, cartão magnético entre outros.

O referido sistema de autenticação deve registrar o nome do usuário, data e hora de acesso, e ser passível de auditoria.

As visitas ao Data Center não autorizadas ocorrerão em caráter de exceção e mediante solicitação de autorização através de fluxo do Sistema ITSM - “Serviço de Acompanhamento de Visitas”, devendo seu acesso e trânsito no Data Center ocorrer, em qualquer ocasião, sob supervisão de empregado autorizado da Área de Hospedagem, conforme estabelece a Norma NP-25.03 - Acesso Físico ao Data Center.

Deverão ser observadas todas as restrições referentes ao acesso, conforme estabelece a Norma NP-25.03.

A entrada ou retirada de quaisquer equipamentos do Data Center somente se dará com o preenchimento, pelo empregado solicitante, do Formulário de Solicitação de Liberação de Equipamento do Data Center, e a autorização formal dos gerentes responsáveis da Superintendência de Operações do Data Center.

9. TRATAMENTO DE DADOS PESSOAIS

O tratamento dos dados pessoais deve atender os requisitos apresentado nesta PSI&P. Todo tratamento de dados pessoais deve ser formalmente autorizado pelo Titular ou orientado pelo Controlador.

9.1 Publicização (Transparência) dos Tratamentos de Dados Pessoais

Os tratamentos de dados pessoais realizados pela PRODESP, quando na posição de Controladora, devem ser publicados nos sistemas desenvolvidos pela empresa, ou em endereço específico determinado pela empresa, para atender aos critérios de transparência exigidos pelas leis gerais de proteção de dados.

9.2 Demandas dos Titulares de Dados

As demandas dos titulares de dados em que a PRODESP atua como Controladora devem ser encaminhados ao Encarregado de Dados da PRODESP por meio do Sem Papel ou e-mail, conforme fluxo divulgado na Intranet na página da PGC, a quem compete a análise e encaminhamento do pedido à área ou profissional responsável pelo seu atendimento.

O encaminhamento do pedido não libera o Encarregado da obrigação de acompanhar e fiscalizar o atendimento das demandas.

9.3 Descarte/Arquivamento de Mídias e Dados

Ao término do Contrato, Termo ou Acordo que envolva tratamento de dados pessoais ou não, e cumprido os prazos da Tabela de Temporalidade da PRODESP e condições do respectivo instrumento legal, as informações serão descartadas de maneira segura e que impeça sua recuperação, ou devolvidos para os respectivos Titulares ou Controladores.

No que se refere a descarte de mídias a Norma NP 25.11 deve ser consultada para que seja dado o tratamento adequado.

10. CONTINUIDADE DO USO DA INFORMAÇÃO E DOS DADOS PESSOAIS

10.1 Da Cópia de Segurança

Toda informação e dado pessoal utilizados para o funcionamento da PRODESP deve possuir, pelo menos, uma cópia de segurança atualizada e guardada em local seguro, com proteção equivalente ao local principal. Esta informação deve ser suficiente para a existência de planos de continuidade de negócio.

No caso de informações e dados pessoais de clientes, as cópias de segurança devem seguir estritamente o previsto em contrato, ou acordado em outro instrumento, com validade legal e aceito pela contratante.

A criação das cópias de segurança deve considerar os aspectos legais, históricos, de auditoria e de recuperação do ambiente.

Os recursos tecnológicos, de infraestrutura e os ambientes físicos onde são realizadas as atividades operacionais do negócio da PRODESP devem ser protegidos contra situações de indisponibilidade, além de estarem abarcados pelo Plano de Contingência e Continuidade da empresa, conforme abaixo elucidado.

10.2 Plano de Contingência e Continuidade

A PRODESP possui um Plano de Contingência e Continuidade baseado na análise de riscos onde leva em consideração a categorização dos Sistemas e Infraestrutura que os suporta definidos como: Hipercríticos, Muito Críticos e Críticos. Este Plano deve ser revisado e atualizado anualmente pelas áreas envolvidas e a documentação gerada deve ser controlada pela Assessoria de Gestão da Qualidade. Este Plano deve sofrer auditoria periódica para validar as atualizações e evidências apresentadas garantindo que os principais sistemas e serviços implantados são testados, no mínimo, anualmente, visando reduzir riscos de perda de confidencialidade, integridade e disponibilidade dos ativos de informação e de dados pessoais.

11. DA DOCUMENTAÇÃO

Todas as Normas e os Procedimentos que possibilitam a proteção da informação e a continuidade do seu uso devem ser documentados, de modo a permitir a continuidade das atividades relacionadas, na hipótese de interrupção, temporária ou definitiva, da relação do usuário com a PRODESP. As Normas deverão ser publicadas na Intranet da PRODESP de forma que qualquer empregado possa ter acesso as mesmas. Já os Procedimentos deverão ser documentados e acessados por todos os empregados que tenham ação de forma a atuar preditivamente ou de forma reativa para sanar qualquer tentativa de ataque ou para realizar investigação em razão de algum ataque sofrido, neste caso os documentos ficarão acessíveis através de diretórios associados a respectivas áreas.

12. INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Qualquer suspeita ou ocorrência de incidente de segurança da informação, como invasões, vazamentos, roubos, sequestros ou tratamentos de informações não autorizados ou fora dos limites autorizados, em equipamentos da empresa ou pessoais, portáteis ou não, deve

ser registrada pelo preenchimento de Formulário de Incidente de Segurança da Informação, disponível na intranet no link https://intranetprodesp-governosp.msappproxy.net/intranet/contact/incidente-de-seguranca, para análise e providências.

O incidente que afete a segurança ou privacidade de dados pessoais deverá ser automaticamente (ou imediatamente) encaminhado ao Encarregado conforme fluxo estabelecido no link https://intranetprodesp-governosp.msappproxy.net/intranet/sites/default/files/tmp/fluxo_documental_-_resposta_incidentes_de_seguranca_-_lgpd_v08.pdf

O registro do incidente poderá ser encaminhado ao Comitê de Segurança da Informação para análise e deliberação.

Todos os requisitos de segurança da informação e de privacidade de dados pessoais, incluindo a necessidade de planos de contingência, devem ser identificados na fase de levantamento de escopo de um projeto ou sistema, e justificados, acordados, documentados, implantados e testados durante a fase de execução.

13. GESTÃO DE RISCOS E CONTROLE INTERNO NAS ÁREAS

Como primeira linha de defesa, todas as áreas são responsáveis pelo mapeamento, classificação, cadastramento e gestão dos seus riscos e de seus controles internos, devendo providenciar o registro deles no sistema SIP da PRODESP.

As áreas devem elaborar e monitorar os Planos de Ação para mitigação dos riscos classificados como Não Aceitáveis.

As gerências devem ter ciência e realizar a gestão dos riscos e controles das suas áreas, assim como, as superintendências para suas gerências, e as diretorias para suas superintendências.

14. FISCALIZAÇÃO E MONITORAMENTO

A fim de verificar o cumprimento, pelos públicos abrangidos por esta PSI&P, dos seus termos e das demais regras e procedimentos aplicáveis, a PRODESP adota procedimentos ativos de fiscalização e monitoramento daqueles que atuam em seu nome ou em seu favor, incluindo:

- Monitoramento e inspeção de todas as comunicações digitais, incluindo e-mails e conexões da Internet e Intranet;
- Inspeção física nas máquinas de sua propriedade;
- Instalação de sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso;
- Fiscalização e monitoramento de todos os perímetros físicos da empresa;
- Registro de entrada e saída de áreas protegidos por dispositivos de controle de acesso, todas as entradas e saídas deverão ser registradas.

15. DO SIGILO DAS INFORMAÇÕES OBTIDAS EM MONITORAMENTO E AUDITORIA

A Gerência de Auditoria poderá retirar o sigilo das informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial, solicitação da Diretoria Executiva ou por determinação do Comitê de Segurança da Informação.

16. TREINAMENTO

Os empregados receberão treinamento sobre o conteúdo desta PSI&P, que ocorrerá em até 30 dias do início das atividades na PRODESP e sempre que o conteúdo for alterado. Sendo assim, o processo de treinamento inicial e o programa de reciclagem continuada são desenvolvidos e controlados pela Gerência de Recursos Humanos exigindo-se comprometimento total dos empregados quanto a sua assiduidade e dedicação, de modo que a participação nos treinamentos possui caráter obrigatório.

A periodicidade mínima do processo de reciclagem continuada será anual. Empregados que, eventualmente, tenham infringido as disposições desta PSI&P e, como medida disciplinar, estejam obrigados a realizar treinamento de reciclagem, não estão isentos da participação dos treinamentos anuais programados para toda a organização.

17. CANAIS DE COMUNICAÇÃO

O conhecimento ou suspeita de violação das diretrizes desta PSI&P devem ser comunicadas ao superior imediato ou registradas no Canal de Denúncias da PRODESP, disponível em https://www.canaldedenuncias.prodesp.sp.gov.br/.

Caso a infração resulte, ou possa resultar, no acesso a dados pessoais controlados ou operados pela PRODESP, entre em contato com o Encarregado de Dados conforme contato publicado na intranet.

Para o registro de reclamações, dúvida, comentário, sugestão ou elogio sobre os serviços prestados pela PRODESP e pelo Poupatempo, acesse a Ouvidoria, pelos links constantes abaixo, e no campo “assunto” escreva Política de Segurança e Privacidade.

Para fala com o Ouvidor PRODESP:
https://www.sgmc.poupatempo.sp.gov.br/formularioeletronicoouvidoria.aspx

Para falar com o Ouvidor Poupatempo:
https://www.sgmc.poupatempo.sp.gov.br/formularioeletronicoouvidoriapoupatempo.aspx

18. VIOLAÇÕES DA POLÍTICA

O não cumprimento desta PSI&P, e procedimentos relacionados, resultará na instauração, caso o infrator seja um empregado, de processo administrativo disciplinar, para apuração da gravidade da violação e, eventualmente, aplicação das penalidades administrativas conforme Código de Conduta e Integridade da PRODESP, além de outras medidas legais.

A violação por fornecedor ou parceiro de negócios observará o disposto em contrato, termo ou acordo, além do previsto nas leis aplicáveis.

As penalidades decorrentes da violação das diretrizes desta PSI&P serão definidas e aplicadas pelo Comitê de Ética da PRODESP, em qualquer caso, garantido ao empregado amplo direito de defesa.

Poderão ser aplicadas (i) aos empregados, entre outras, penas de advertência, obrigação de realização de treinamento de reciclagem, suspensão, desligamento ou demissão por justa causa, se aplicável, nos termos da legislação vigente no país à época do fato; (ii) aos fornecedores e parceiros de negócios, pena pecuniária, conforme disposto em contrato, termo ou acordo. Referidas penalidades serão aplicadas sem prejuízo do direito da PRODESP de pleitear direito de regresso, indenização pelos eventuais prejuízos suportados, perdas e danos e/ou lucros cessantes, por meio das diligências legais cabíveis.

19. REVISÃO DA POLÍTICA

Esta PSI&P e seus procedimentos complementares, deverão ser revistos e atualizados a cada dois anos ou sempre que algum fato relevante motive sua revisão antecipada, conforme análise e decisão do Comitê de Segurança.