ANEXO E - - Relatório de Impacto à Proteção de Dados Pessoais

O presente anexo traz explicações a respeito da utilização da tecnologia no Programa Smart Sampa de forma detalhada com o intuito de tranquilizar, esclarecer e informar com relação a segurança, privacidade e utilização da tecnologia para monitoramento que deverá estar disponível na nova plataforma. Entendendo ser necessário demonstrar a utilização da Plataforma Smart Sampa e o compromisso com a população garantindo o compliance com a legislação vigente e interesse público afastando qualquer dúvida quanto à Implantação e Utilização da Plataforma Smart Sampa como parte das políticas de públicas de integração, cooperação, interoperabilidade dos serviços Municipais e de Governo Digital.

1. Análise de riscos à Proteção de Dados Pessoais

Este relatório de impacto à proteção de dados pessoais tem como objetivo avaliar os riscos e identificar as medidas necessárias para garantir a conformidade com a Lei Geral de Proteção de Dados (LGPD) no contexto de um sistema de videomonitoramento com inteligência artificial embarcada e reconhecimento facial implementado por órgão público no âmbito da segurança pública.

1.1. Identificação dos dados pessoais coletados e armazenados

O sistema de videomonitoramento com inteligência artificial embarcada e reconhecimento facial coleta e armazena os seguintes dados pessoais: (i) Imagens de vídeo com reconhecimento facial; (ii) Data e hora da coleta das imagens. Esses dados são coletados para fins de segurança pública e são armazenados em servidores do órgão público responsável pelo sistema.

1.2. Avaliação dos riscos

Em seguida, avaliamos os riscos envolvidos na coleta e armazenamento desses dados pessoais. Identificamos os seguintes riscos: (i) possibilidade de coleta de dados pessoais sem o consentimento dos indivíduos; (ii) uso indevido dos dados pessoais coletados; (iii) falhas de segurança que permitam acesso não autorizado às imagens coletadas; (iv) possibilidade de discriminação ou preconceito no reconhecimento facial; (v) falta de transparência no uso dos dados coletados; (vi) possibilidade de vazamento de dados pessoais.

1.3. Medidas de proteção dos dados pessoais

Para mitigar os riscos identificados, a PARCEIRA implementará as seguintes medidas de proteção dos dados pessoais, considerando normas ISO relevantes:

(i) Coleta de dados pessoais apenas para fins específicos e legítimos relacionados à segurança pública, em conformidade com a LGPD (13.709/2018) e ISO 27701:2019 - Privacidade da Informação - Extensão à ISO/IEC 27001 e ISO/IEC 27002;

(ii) Obtenção de consentimento dos indivíduos em caso de coleta de dados pessoais sensíveis, de acordo com a ISO/IEC 29100:2011 - Tecnologias da Informação - Privacidade e Proteção de Dados Pessoais - Estrutura e Princípios Gerais, seguindo a LGPD (13.709/2018) e as exceções nela descritas para fins de segurança pública;

(iii) Utilização de criptografia para proteção dos dados pessoais armazenados, seguindo as recomendações da ISO/IEC 27002:2013 - Tecnologia da Informação - Técnicas de Segurança - Código de Prática para Controles de Segurança da Informação;

(iv) Implementação de políticas de segurança da informação para prevenção de acessos não autorizados e monitoramento constante da rede e sistemas, em conformidade com a ISO/IEC 27001:2013 - Tecnologia da Informação - Técnicas de Segurança - Sistemas de Gestão de Segurança da Informação - Requisitos;

(v) Restrição de acesso aos dados pessoais apenas aos funcionários autorizados e treinados sobre a importância da proteção de dados pessoais, seguindo as recomendações da ISO/IEC 27002:2013 - Tecnologia da Informação - Técnicas de Segurança - Código de Prática para Controles de Segurança da Informação;

(vi) Transparência no uso dos dados coletados e disponibilização de informações claras sobre a finalidade do sistema de monitoramento, em conformidade com a ISO/IEC 29100:2011 - Tecnologias da Informação - Privacidade e Proteção de Dados Pessoais - Estrutura e Princípios Gerais;

(vii) Implementação de um processo de avaliação de impacto à proteção de dados pessoais em conformidade com a ISO/IEC 29134:2017 - Tecnologia da Informação - Técnicas de Segurança - Técnicas para a Avaliação de Privacidade e Impacto à Proteção de Dados.

1.4. Conclusão

A implementação de um sistema de vídeo monitoramento com inteligência artificial embarcada e reconhecimento facial por órgão público no âmbito da segurança pública envolve riscos significativos à proteção de dados pessoais. No entanto,

medidas de proteção podem ser implementadas para mitigar esses riscos, garantindo a conformidade com a LGPD e normas ISO relevantes.

É importante destacar a importância da transparência no uso desses dados e a necessidade de se garantir que os indivíduos sejam informados sobre a coleta e o processamento de seus dados pessoais. Além disso, é fundamental que o órgão público responsável pelo sistema de videomonitoramento esteja preparado para lidar com possíveis incidentes de segurança da informação, bem como com as solicitações de acesso e correção de dados pessoais pelos indivíduos afetados.

Referências Normativas:

(i) ISO 27701:2019 - Privacidade da Informação - Extensão à ISO/IEC 27001 e ISO/IEC 27002;
(ii) ISO/IEC 29100:2011 - Tecnologias da Informação - Privacidade e Proteção de Dados Pessoais - Estrutura e Princípios Gerais;
(iii) ISO/IEC 27002:2013 - Tecnologia da Informação - Técnicas de Segurança - Código de Prática para Controles de Segurança da Informação;
(iv) ISO/IEC 27001:2013 - Tecnologia da Informação - Técnicas de Segurança - Sistemas de Gestão de Segurança da Informação - Requisitos;
(v) ISO/IEC 29134:2017 - Tecnologia da Informação - Técnicas de Segurança - Técnicas para a Avaliação de Privacidade e Impacto à Proteção de Dados.

2. Matriz de Risco a Proteção de Dados

	Probabilidade Alta	**Probabilidade Média**	**Probabilidade Baixa**
Impacto Alto	Acesso não autorizado a dados pessoais (Risco Médio)	Uso indevido de dados pessoais (Risco Médio)	Violação da privacidade de indivíduos (Risco Médio)
	Falhas de segurança que permitem o acesso não autorizado a dados pessoais (Risco Alto)	Falhas no reconhecimento facial que podem levar à identificação	Interrupção ou indisponibilidade do sistema de videomonitoramento (Risco Baixo)

		equivocada de indivíduos (Risco Médio)	
Impacto Médio	Interrupção ou indisponibilidade do sistema de videomonitoramento (Risco Médio)	Violação da privacidade de indivíduos (Risco Médio)	Uso indevido de dados pessoais (Risco Baixo)
	Falhas de segurança que permitem o acesso não autorizado a dados pessoais (Risco Médio)	Falhas no reconhecimento facial que podem levar à identificação equivocada de indivíduos (Risco Baixo)	-
Impacto Baixo	Interrupção ou indisponibilidade do sistema de videomonitoramento (Risco Baixo)	-	-

A probabilidade de cada risco ser alto, médio ou baixo foi determinada com base na avaliação dos controles existentes para mitigar o risco, bem como a frequência e impacto de incidentes anteriores similares.

A seguir, são fornecidas mais informações sobre cada risco e as medidas de proteção recomendadas para mitigá-los:

2.1. Acesso não autorizado a dados pessoais

(i) Probabilidade alta: Existe um alto risco de acesso não autorizado a dados pessoais devido a falhas de segurança no sistema de vídeo monitoramento.

(ii) Probabilidade média: Existe uma probabilidade média de acesso não autorizado a dados pessoais.

(iii) Probabilidade baixa: A probabilidade de acesso não autorizado a dados pessoais é baixa devido à presença de medidas de segurança adequadas, como autenticação forte e controles de acesso.

2.1.1. Medidas de proteção recomendadas:

(i) Implementação de controles de acesso para garantir que apenas pessoas autorizadas tenham acesso aos dados pessoais.
(ii) Uso de autenticação forte, como autenticação de dois fatores, para impedir que pessoas não autorizadas acessem o sistema.
(iii) Implementação de criptografia de dados para garantir que os dados pessoais permaneçam seguros, mesmo se houver acesso não autorizado.

2.2. Uso indevido de dados pessoais

(i) Probabilidade alta: Existe um alto risco de uso indevido de dados pessoais devido a possíveis falhas no treinamento da inteligência artificial e do reconhecimento facial.
(ii) Probabilidade média: Existe uma probabilidade média de uso indevido de dados pessoais.
(iii) Probabilidade baixa: A probabilidade de uso indevido de dados pessoais é baixa devido à existência de políticas e procedimentos adequados para garantir o uso adequado dos dados.

2.2.1. Medidas de proteção recomendadas:

(i) Implementação de políticas e procedimentos claros para garantir que os dados pessoais sejam usados apenas para fins legítimos e autorizados.
(ii) Treinamento adequado de pessoal para garantir que os dados pessoais sejam manuseados de acordo com as políticas e procedimentos estabelecidos.
(iii) Implementação de auditorias regulares para garantir que o uso de dados pessoais esteja em conformidade com as políticas e procedimentos estabelecidos.

2.3. Violação da privacidade de indivíduos

(i) Probabilidade alta: Existe um alto risco de violação da privacidade de indivíduos devido a falhas de segurança no sistema de vídeo monitoramento.

(ii) Probabilidade média: Existe uma probabilidade média de violação da privacidade de indivíduos.

(iii) Probabilidade baixa: A probabilidade de violação da privacidade de indivíduos é baixa devido à existência de medidas de proteção adequadas, como criptografia de dados e controles de acesso.

2.3.1. Medidas de proteção recomendadas:

(i) Implementação de políticas e procedimentos claros para garantir que a privacidade dos indivíduos seja respeitada.

(ii) Uso de criptografia de dados para garantir que os dados pessoais permaneçam seguros.

(iii) Implementação de controles de acesso para garantir que apenas pessoas autorizadas tenham acesso aos dados pessoais.

2.4. Falhas de segurança que permitem o acesso não autorizado a dados pessoais.

(i) Probabilidade alta: Existe um alto risco de falhas de segurança que permitam o acesso não autorizado a dados pessoais.

(ii) Probabilidade média: Existe uma probabilidade média de falhas de segurança que permitam o acesso não autorizado a dados pessoais.

(iii) Probabilidade baixa: A probabilidade de falhas de segurança que permitam o acesso não autorizado a dados pessoais é baixa devido à existência de medidas de proteção adequadas.

2.4.1. Medidas de proteção recomendadas:

(i) Implementação de controles de acesso para garantir que apenas pessoas autorizadas tenham acesso aos dados pessoais.

(ii) Uso de autenticação forte para impedir que pessoas não autorizadas acessem o sistema.

(iii) Implementação de criptografia de dados para garantir que os dados pessoais permaneçam seguros.

2.5. Falhas no reconhecimento facial que podem levar à identificação equivocada de indivíduos

(i) Probabilidade alta: Existe um alto risco de falhas no reconhecimento facial que podem levar à identificação equivocada de indivíduos.

(ii) Probabilidade média: Existe uma probabilidade média de falhas no reconhecimento facial que podem levar à identificação equivocada de indivíduos.

(iii) Probabilidade baixa: A probabilidade de falhas no reconhecimento facial que podem levar à identificação equivocada de indivíduos é baixa devido à existência de medidas de proteção adequadas.

2.5.1. Medidas de proteção recomendadas:

(i) Implementação de testes regulares para garantir a precisão do reconhecimento facial.

(ii) Treinamento adequado da inteligência artificial para garantir a precisão do reconhecimento facial.

(iii) Implementação de políticas e procedimentos claros para lidar com casos em que a identificação equivocada de indivíduos ocorra.

2.6. Com base na matriz de risco, é recomendado que medidas de proteção adequadas sejam implementadas para mitigar os riscos identificados. Essas medidas incluem a implementação de políticas e procedimentos claros para garantir que os dados pessoais sejam usados apenas para fins legítimos e autorizados, o treinamento adequado de pessoal para lidar com dados pessoais, a implementação de auditorias regulares para garantir a conformidade com as políticas e procedimentos estabelecidos, o uso de criptografia de dados para garantir que os dados pessoais permaneçam seguros, a implementação de controles de acesso para garantir que apenas pessoas autorizadas tenham acesso aos dados pessoais e a implementação de testes regulares para garantir a precisão do reconhecimento facial.

2.7. Essas medidas de proteção devem ser baseadas nas normas ISO 27001 e ISO 27701, que fornecem orientações sobre a implementação de um sistema de gestão de segurança da informação e um sistema de gestão de privacidade de informações pessoais, respectivamente. Essas normas ajudam a garantir que as medidas de proteção implementadas sejam adequadas e eficazes.

2.8. Além disso, é importante que uma avaliação de impacto à proteção de dados seja realizada regularmente para garantir que o sistema de videomonitoramento continue a ser compatível com as normas de proteção de dados pessoais e para identificar novos riscos à privacidade dos indivíduos.

3. Compliance e das Garantias

3.1 Necessidades e Garantias

A necessidade de assegurar as garantias básicas a direitos fundamentais, por ela afetados e suas normas correspondentes – em especial, os direitos de imagem, de privacidade e de proteção de dados pessoais, desta forma além de já prever mecanismos para garantir estes direitos, o programa é plenamente aderente a possíveis regulações posteriores pela ANPD (Agência Nacional de Proteção de Dados), podendo se adequar a novos processos, fluxos e tecnologias de proteção de dados e privacidade.

3.2 Dados Armazenados e Privacidade

A utilização da solução deve seguir as diretrizes e finalidades do Programa Smart Sampa, sendo vedada qualquer utilização fora do escopo aprovado, garantindo a privacidade e proteção dos dados pessoais. Os controles de acessos e privilégios de usuário devem impedir qualquer acesso ou uso fora do especificado, considerado invasivo/desnecessário a atividade e escopo do Programa Smart Sampa. Todo dado armazenado deve ser criptografado e dados que não são de interesse do poder público, sem requisição de qualquer órgão será eliminada em 30 dias, incluindo as imagens e dados biométricos limitando o volume de dados armazenados. Qualquer imagem, dado ou informação, só poderá sair do sistema, ser enviada ou cedida mediante solicitação oficial de órgão competente conforme legislação vigente, não sendo divulgada, veiculada ou utilizada para qualquer outro fim além dos previstos legalmente. Evitando assim a exposição desnecessária de pessoas e a invasão à privacidade, tendo em vista que a finalidade das imagens e dados captados não é a invasão à privacidade, mas sim melhorar os serviços oferecidos e a segurança no Município.

3.3 Acompanhamento contínuo dos resultados

Deve ser monitorado durante o seu continuum, por meio de uma Avaliação de Resultado da implementação, assim como das políticas públicas suportadas pelo programa, a fim de avaliar os resultados de seu objetivo e a correspondência entre as análises prévias sobre o impacto e seus efeitos com a realidade concretamente observada e documentada. Conforme já definido, toda e qualquer projeto passará regularmente a cada 6 meses por revisões, sendo analisado todos os impactos, eficiência e alinhamento, com as

expectativas prévias sendo todo o processo documentado, incluindo todos os ajustes de processos e procedimentos realizados pelos agentes. Qualquer variação de resultado positivo ou negativo será possível corrigir, como qualquer intercorrência, que incline o programa em direção diferente da definida como referência. Sendo um processo de melhoria constante dos sistemas que compõem a Plataforma, assim como tudo que compõem o Programa Smart Sampa, com metodologias tais como PDCA, six sigma, 5S, BSC, entre outros utilizados para fazer a gestão e revisões constantes, em todos os aspectos do programa, incluindo a solução tecnológica adotada para garantir o alinhamento da tecnologia aos interesses públicos, sendo todos os resultados avaliados e publicados no portal da transparência e demais canais a cada ciclo.

3.3.1. Tratamento de Dados

Deve ser pública a descrição do contexto, da natureza, do escopo, da necessidade e da finalidade do tratamento das categorias de dados pessoais (art. 5º, inc. I, LGPD) e de dados pessoais sensíveis (art. 5º, inc. II, LGPD), envolvidas no Programa disponibilizadas através do portal da transparência e demais canais da Prefeitura Municipal de São Paulo, deixando clara a forma como os dados serão captados, tratados, processados, armazenados e eliminados, com exemplos claros da utilização e simplificando o entendimento do processo e utilização da tecnologia. Exemplo de dados utilizados: (i) dados de Atendimento; (ii) dados de Identificação; (iii) Dados Biométricos (iv) Características; (v) Contextos e Ações; (vi) Dados e Documentos relacionados

3.3.2. Segurança do Programa Smart Sampa

Será instituído como padrão nos serviços, integrações, cooperações e qualquer outra atividade ligada direta ou indiretamente ao Programa Smart Sampa, os parâmetros definidos a partir dos documentos abaixo:

(i) Estrutura Organizacional
(ii) Política de Segurança da Informação
(iii) Política de Segurança Cibernética
(iv) Política de Transparência e Compliance
(v) Política de Privacidade (Usuários finais)
(vi) Política de Proteção de Dados e Privacidade (Uso Interno)
(vii) Política de Integridade e ética
(viii) Padrões, Processos e Procedimentos operacionais

(ix) Mapa de Riscos e Impactos
(x) Relatório de Impacto à Proteção de dados pessoais
(xi) Categorização dos dados, informações e ciclo de vida
(xii) Plano de Gestão das Hipóteses de Tratamento de dados pessoais
(xiii) Plano de Mitigação de Riscos
(xiv) Plano de Resposta a Incidentes
(xv) Plano de Recuperação de Desastres
(xvi) Plano de Contingência

Estes documentos devem ser desenvolvidos em conjunto, mas especialmente da PARCERIA, tendo em vista às variações de tecnologia e processos que serão adotados, sendo assim necessário alinhamento. Não sendo possível defini-los sem o entendimento entre o provedor de serviços (PARCERIA) e operador (PRODAM). O desenvolvimento desses documentos é necessário para estabelecer as normas e processos para a operação da plataforma no dia a dia e previsão e prevenção de eventuais eventos adversos.

Esses documentos serão elaborados logo após a instalação do projeto, após 3 meses da assinatura do contrato, trazendo assim maior efetividade na segurança e transparência do Programa Smart Sampa como um todo

4. Utilização da Plataforma e Tratamento de Dados

4.1 Apenas órgãos do poder público contratante poderão operar a Plataforma Smart Sampa, tendo acesso aos seus dados e processos. A PARCEIRA não terá acesso a dados sensíveis ou sigilosos. Em casos excepcionais onde exista a necessidade de acesso durante a implementação, o conselho de gestão da plataforma irá deliberar sobre a autorização dos envolvidos, que deverão assinar termo de sigilo e confidencialidade, desenvolvido especificamente para a atividade desempenhada, devendo estes estar sempre acompanhados de um fiscal da PRODAM durante toda a implementação.

4.2. Tão logo os documentos desse RIPD estejam prontos e aprovados, serão encaminhados para conhecimento do encarregado de dados e do controle interno do órgão público.

4.3. Será observado o compartilhamento de dados com propósitos legítimos, específicos e explícitos, limitando ao mínimo necessário para o atendimento das finalidades do programa. Em observância ao o julgamento conjunto da Ação Direta de Inconstitucionalidade nº 6.649/DF e da Arguição de Descumprimento de Preceito Fundamental nº 695/DF.

4.4. O compartilhamento de informações pessoais em atividades de inteligência, observará adoção de medidas estritamente necessárias ao atendimento do interesse público, podendo ter acompanhamento do poder judiciário, com estrito controle de acesso.

4.5. Do registro das operações

A Plataforma deverá manter o registro das operações de tratamento de dados pessoais realizadas. Para cumprir com esta obrigação, esta etapa objetiva identificar os processos do tratamento de dados pessoais, os fluxos e ciclos de vida desses dados dentro e fora do programa (informações acessadas, coletadas, usadas, transferidas, armazenadas ou compartilhadas), em conformidade ao artigo 37 da LGPD.

4.5.1. Os controladores e operadores realizarão e manterão o registro das operações com a devida associação das bases legais, em especial quando for o legítimo interesse, desta forma poderá ser solicitado pela autoridade nacional de proteção de dados (ANPD).

4.5.2. Todos os processos e atividades desenvolvidas ou relacionadas ao Programa Smart Sampa, serão documentadas com o intuito de trazer garantias e demonstrar a efetividade da governança adotada, em privacidade, transparência, boas práticas, processos, códigos de condutas e todas as outras medidas para o cumprimento da legislação.

4.5.3. Desta forma todo o Programa Smart Sampa poderá ser auditado quando necessário, para demonstrar a efetividade das medidas adotadas, objetivos almejados e resultados obtidos. Mostrando de forma cronológica todas as alterações e adequações realizadas ao longo do Programa, para atender as regulamentações e legislação vigente, conforme LGPD em seus artigos 37, 38, 46, 47, 48, 49 e 50. Que exige controle, governança e transparência no processamento de dados, identificando a natureza, necessidade, objetivos e riscos do tratamento de dados realizado.

4.6. Canal de Comunicação

Será criado um canal de comunicação web site pelo Controlador órgão público ao CRM para atendimento aos titulares dos dados onde os usuários da plataforma poderão solicitar informações referentes ao tratamento dos seus dados pessoais e terão acessos aos controladores das informações, conforme dispõe os artigos 9º, 17º e 22º todos da Lei 13.709 de 14 de 08/2018 (LGPD) de

forma que os titulares dos dados possam esclarecer dúvidas e entender o processamento dos dados.

4.6.1. Terá a devida publicidade realizada em eventual site do programa e nos canais de comunicação do órgão público, bem como em peças publicitárias da municipalidade.

4.6.2. A plataforma Smart Sampa desde sua implementação deverá fornecer informações de operação que serão disponibilizadas no portal da transparência do órgão público, incluindo impacto e resultados.

4.6.3. O tratamento de dados de idosos deverá ser efetuado de maneira simples, clara, acessível e adequada ao seu entendimento. Garantindo a inclusão da terceira idade nas políticas públicas que utilizam tecnologia e tratamento de dados em seus processos, tendo pleno conhecimento da utilização da de seus dados e as hipóteses em que são processados e com qual objetivo. Garantindo igualdade de acesso e compreensão cumprindo o Estatuto do Idoso Lei nº 10.741, de 1º de outubro de 2003, e as diretrizes da Agência Nacional de Proteção de Dados Lei 13.853 de 2019, dando atenção especial ao disposto no Art. 55-J inciso XIX da Lei 13.853.

5. Compliance do Programa na utilização da tecnologia e processos adotados

O Chefe de Equipe de Fiscalização e Compliance da PARCEIRA deverá fornecer aos operadores e seus internos orientações sobre o tratamento de dados pessoais, além de garantir que todos os operadores possuam o devido treinamento para operação da plataforma e tratamento de dados. Fazendo requalificação de pessoal sempre que necessário.

5.1. O Chefe de Equipe de fiscalização e compliance ficará encarregado de fiscalizar os processos, a utilização da plataforma e o Compliance (fazer cumprir todas as políticas, normas, processos adotados e legislação vigente). Os processos e soluções adotados devem mitigar impactos aos direitos individuais e trazer garantias de privacidade, segurança e transparência, tornando a tecnologia menos invasiva na captura de dados e não deixando estas informações disponíveis aos operadores sem que exista necessidade. Devendo a utilização ser aprovada pelo Chefe de Equipe de Fiscalização e Compliance e mantendo todos os dados armazenados criptografados.

5.2 Para uso interno será instituída a Política de Proteção de Dados e Privacidade, trazendo as diretrizes sobre sigilo e privacidade, além de punições administrativas cabíveis, a desvios dos Servidores Públicos no ato de suas

funções. Dispondo sobre as práticas adotadas com relação à privacidade e à proteção de dados pessoais no âmbito do Programa, contendo todo o detalhamento necessário ao entendimento com exemplos do que é permitido e do que não é, conforme as melhores prática e legislação vigente.

5.3. No caso de criação de site vinculado ao projeto, atualmente, não é prevista a utilização de websites ou Cookies no programa voltados aos usuários finais (munícipes etc), devido aos vários canais utilizados para comunicação já existentes (portal da transparência, capital.sp.gov.br e outros endereços da PMSP). Em caso de futura implantação de websites e Cookies voltados ao programa, este seguirá toda a legislação vigente, incluindo aviso de Privacidade, política de privacidade, exibindo a notificação com a política de Cookies e rastreabilidade dos usuários entre outros mecanismos que visam garantir a privacidade dos usuários ao utilizar sites e aplicativos.

6. Parametrização dos Analiticos e Processos

6.1. Parâmetro para gerar alertas automáticos A plataforma só deve produzir alertas quando a análise dos analíticos for de maior ou igual a 90% de paridade. Todo e qualquer evento em que o analítico esteja menor a 90% será automaticamente descartado.

6.2. Todos os alertas gerados ficarão armazenados, para análise e revisão dos processos de tratamento e tomada de decisão, com o intuito de garantir eficiência e o aprimoramento do processo.

7. Da Utilização da Plataforma

7.1. A Plataforma Smart Sampa deve suportar a operação de forma eficiente, segura e transparente, seguindo a política de segurança da informação vigente, que será atualizada sempre que se mostre necessário. A solução deve manter histórico detalhado de tudo que ocorrer na plataforma, incluindo atividade dos operadores e agentes. Deve possuir sistema robusto de controle, níveis de acesso, permissões e privilégios. Sendo gerido de forma unificada servindo tanto para controle e acesso da plataforma, como para dar acesso aos espaços físicos dos centros (Centro Operacional e Centro Administrativo) que se fizerem necessários, onde o controle de acesso estará instalado.