AGÊNCIA DE ASSUNTOS METROPOLITANOS DO PARANÁ - AMEP

EDITAL E MODELO DE SELEÇÃO PARA DELEGAÇÃO DO SISTEMA DE TRANSPORTE PÚBLICO DE PASSAGEIROS DA REGIÃO METROPOLITANA DE CURITIBA, MATERIAL RODANTE SOBRE PNEUS

11. ANEXO XI – POLÍTICA DE GOVERNANÇA DE DADOS E SEGURANÇA

CURITIBA

JULHO /2026

ÍNDICE

AGÊNCIA DE ASSUNTOS METROPOLITANOS DO PARANÁ – AMEP
Palácio das Araucárias – Rua Jacy Loureiro de Campos, s/n – 1º andar – Centro Cívico – CEP 80.530-140 – Curitiba – Paraná
(41) 3320 6900 I www.amep.pr.gov.br

AGÊNCIA DE ASSUNTOS METROPOLITANOS DO PARANÁ – AMEP
Palácio das Araucárias – Rua Jacy Loureiro de Campos, s/n – 1º andar – Centro Cívico – CEP 80.530-140 – Curitiba – Paraná
(41) 3320 6900 I www.amep.pr.gov.br

AGÊNCIA DE ASSUNTOS METROPOLITANOS DO PARANÁ – AMEP
Palácio das Araucárias – Rua Jacy Loureiro de Campos, s/n – 1º andar – Centro Cívico – CEP 80.530-140 – Curitiba – Paraná
(41) 3320 6900 I www.amep.pr.gov.br

AGÊNCIA DE ASSUNTOS METROPOLITANOS DO PARANÁ – AMEP
Palácio das Araucárias – Rua Jacy Loureiro de Campos, s/n – 1º andar – Centro Cívico – CEP 80.530-140 – Curitiba – Paraná
(41) 3320 6900 I www.amep.pr.gov.br

AGÊNCIA DE ASSUNTOS METROPOLITANOS DO PARANÁ – AMEP
Palácio das Araucárias – Rua Jacy Loureiro de Campos, s/n – 1º andar – Centro Cívico – CEP 80.530-140 – Curitiba – Paraná
(41) 3320 6900 I www.amep.pr.gov.br

CONDIÇÕES GERAIS

1. OBJETIVO

Garantir que a Política de Governança de Dados e Segurança esteja plenamente alinhada às melhores práticas estabelecidas pelo NIST Cybersecurity Framework (CSF), incluindo a metodologia de Risk Rating Score, bem como à legislação vigente — em especial o Decreto nº 2009/2015 — assegurando sua aplicação nos sistemas e demais elementos de Tecnologia da Informação e Comunicação do Sistema de Transporte Público de Passageiros da Região Metropolitana de Curitiba – **TIC do STPP/RMC**;

Proteger os dados, garantindo que as informações integrantes do patrimônio e aquelas sob guarda do Sistema de Transporte Público de Passageiros da Região Metropolitana de Curitiba – **STPP/RMC**, assim como as ferramentas utilizadas para obtenção, geração, modificação, armazenagem e disponibilização delas estejam em conformidade com as leis vigentes no país.

Atender às premissas de segurança da informação observando os pilares: Disponibilidade, Confidencialidade e Integridade.

Nesse contexto, a AMEP, na qualidade de **PODER CONCEDENTE**, estabelece que os concessionários e a Operadora do Sistema de Bilhetagem Eletrônica (**SBE**) devem pautar suas operações pelo estrito cumprimento das diretrizes de segurança da informação. A conformidade não se limita apenas à Lei Geral de Proteção de Dados (LGPD), mas estende-se à adoção de padrões internacionais de excelência, especificamente as normas ISO/IEC 27001 (Sistema de Gestão de Segurança da Informação) e ISO/IEC 27701 (Gestão de Privacidade da Informação).

Para viabilizar essa governança, as políticas internas da **AMEP** servirão como referencial obrigatório para a elaboração dos documentos basilares da concessão, devendo ser observadas a Política de Privacidade de Dados, a Política de Tratamento de Incidentes à Privacidade de Dados e a Política da Classificação de Riscos Relativos à Privacidade dos Dados.

AGÊNCIA DE ASSUNTOS METROPOLITANOS DO PARANÁ – AMEP
Palácio das Araucárias – Rua Jacy Loureiro de Campos, s/n – 1º andar – Centro Cívico – CEP 80.530-140 – Curitiba – Paraná
(41) 3320 6900 I www.amep.pr.gov.br

2. CAMPO DE APLICAÇÃO

Esta Política aplica-se aos sistemas e demais elementos de Tecnologia da Informação e Comunicação, partes integrantes da concessão do Sistema de Transporte Público de Passageiros da Região Metropolitana de Curitiba - **TIC do STPP/RMC**, a todos os Partícipes e aos Usuários da informação. Adicionalmente, aplica-se a qualquer indivíduo, seja ele prestador de serviço, parceiro ou terceiro, que interaja com os sistemas do **STPP**, utilize credenciais de acesso ou que, por qualquer motivo, tenha acesso a informações gerenciadas pelo **STPP**, incluindo dados pessoais.

3. DEFINIÇÕES

Para fins deste ANEXO, considera-se:

3.1. Agentes de TIC do STPP/RMC:

Pessoa jurídica que atue direta ou indiretamente na infraestrutura tecnológica ou correlata do Sistema de Transporte Público de Passageiros da Região Metropolitana de Curitiba - **STPP/RMC**, incluindo, mas não se limitando a: Poder Concedente, Operadoras, Concessionárias, Fornecedoras de Tecnologia, Verificadores de Conformidade e demais parceiros institucionais.

3.2. Autenticidade:

Propriedade que assegura a identificação inequívoca dos elementos envolvidos na troca eletrônica ou não de informações, garantindo que a origem e autoria sejam verificáveis e evitando o repúdio.

3.3. Colaborador:

Pessoa física que possua vínculo empregatício ou de trabalho com qualquer Agente de **TIC** do **STPP/RMC**, atuando conforme normas internas e legislação aplicável.

3.4. Concessionárias:

Delegatária da operação do **STPP/RMC**.

AGÊNCIA DE ASSUNTOS METROPOLITANOS DO PARANÁ – AMEP
Palácio das Araucárias – Rua Jacy Loureiro de Campos, s/n – 1º andar – Centro Cívico – CEP 80.530-140 – Curitiba – Paraná
(41) 3320 6900 I www.amep.pr.gov.br

3.5. Confidencialidade:

Garantia de que a informação é acessível somente a pessoas ou sistemas devidamente autorizados, prevenindo divulgação indevida.

3.6. Controlador:

Pessoa natural ou jurídica, pública ou privada, que toma decisões referentes ao tratamento de dados pessoais, determinando as finalidades e os meios dessa coleta e uso, conforme previsto na Lei Geral de Proteção de Dados (LGPD).

3.7. Custodiante:

Pessoa jurídica que, por força contratual ou regulatória, assume a responsabilidade pela guarda, proteção, manutenção e gestão dos ativos tecnológicos, sistemas, dados e serviços que compõem a infraestrutura de **TIC** do **STPP/RMC**, garantindo conformidade com a Política de Governança de Dados e Segurança, legislação vigente e boas práticas internacionais (como NIST CSF e ISO/IEC 27001).

3.8. Disponibilidade:

Propriedade que assegura que usuários autorizados obtenham acesso às informações e aos ativos correspondentes sempre que necessário, garantindo continuidade operacional.

3.9. Fornecedor:

Pessoa Jurídica que forneça produtos ou serviços a outras empresas, sendo responsável por disponibilizar materiais, mercadorias, equipamentos ou serviços essenciais relacionados ao **STPP/RMC**.

3.10. Fornecedora de Tecnologia:

Pessoa Jurídica parceira ou contratada, responsável pelo desenvolvimenteo, fornecimento, integração, manutenção e/ou suporte técnico de ativos tecnológticos, softwares, infraestrutura de redes e sistemas embarcados essenciais ao funcionamento do **STPP/RMC**.

AGÊNCIA DE ASSUNTOS METROPOLITANOS DO PARANÁ – AMEP
Palácio das Araucárias – Rua Jacy Loureiro de Campos, s/n – 1º andar – Centro Cívico – CEP 80.530-140 – Curitiba – Paraná
(41) 3320 6900 I www.amep.pr.gov.br

3.11. Gestor da Informação:

Indivíduo responsável por decisões estratégicas quanto ao uso, classificação e proteção de informações, garantindo conformidade com políticas internas, legislação e normas aplicáveis.

3.12. Integridade:

Propriedade que assegura a exatidão e a completeza da informação e dos métodos de processamento, prevenindo alterações não autorizadas.

3.13. Legalidade:

Característica que assegura que o tratamento da informação está em conformidade com leis, regulamentos e normas aplicáveis, evitando riscos jurídicos e sanções.

3.14. Operador:

Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do Controlador, conforme previsto na LGPD.

3.15. Poder Concedente:

Agência de Assuntos Metropolitanos do Paraná – **AMEP**, autarquia estadual do Governo do Paraná e Poder Concedente dos serviços públicos de transporte coletivo de passageiros, responsável pela gestão do sistema de transporte metropolitano da Região Metropolitana de Curitiba.

3.16. PSI (Política de Segurança da Informação):

Conjunto de diretrizes, normas e procedimentos que estabelecem requisitos para proteção das informações, garantindo confidencialidade, integridade, disponibilidade e conformidade legal.

3.17. SAU (Serviço de Atendimento ao Usuário):

Parte integrante da infraestrutura de **TIC** do **STPP/RMC** destinada a prestar suporte e atendimento aos usuários, garantindo eficiência e conformidade com normas aplicáveis.

AGÊNCIA DE ASSUNTOS METROPOLITANOS DO PARANÁ – AMEP
Palácio das Araucárias – Rua Jacy Loureiro de Campos, s/n – 1º andar – Centro Cívico – CEP 80.530-140 – Curitiba – Paraná
(41) 3320 6900 I www.amep.pr.gov.br

3.18. SBE (Sistema de Bilhetagem Eletrônica):

Parte integrante da infraestrutura de **TIC** do **STPP/RMC**, responsável pela gestão da bilhetagem eletrônica, incluindo emissão, validação e controle de créditos de transporte, garantindo segurança, disponibilidade e conformidade com normas regulatórias.

3.19. Segurança da Informação:

Conjunto de medidas, controles e políticas que visam proteger as informações contra acesso, uso, divulgação, alteração ou destruição não autorizada, garantindo confidencialidade, integridade, disponibilidade e conformidade legal.

3.20. STPP/RMC:

Sistema de Transporte Público de Passageiros da Região Metropolitana de Curitiba, concedido mediante procedimento licitatório para exploração do serviço de transporte público metropolitano operado por material rodante sobre pneus.

3.21. Usuário da Informação:

Pessoa que interage diretamente com sistemas informatizados, podendo adicionar ou atualizar informações, desde que autorizada. Inclui colaboradores, prestadores de serviço, terceirizados, parceiros, estagiários ou fornecedores com acesso aos bens de informação de **TIC** do **STPP/RMC**.

4. RESPONSABILIDADE

4.1. DO PODER CONCEDENTE

Avaliar e aprovar a Política de Segurança da Informação;

Assegurar que os Agentes de **TIC** do **STPP/RMC** conheçam e cumpram esta Política e/ou a PSI;

Assegurar que a **Política de Governança de Dados e Segurança** e os objetivos estabelecidos são compatíveis com as normas e legislações pertinentes;

Garantir a integração dos requisitos de segurança da informação dentro dos processos de

AGÊNCIA DE ASSUNTOS METROPOLITANOS DO PARANÁ – AMEP
Palácio das Araucárias – Rua Jacy Loureiro de Campos, s/n – 1º andar – Centro Cívico – CEP 80.530-140 – Curitiba – Paraná
(41) 3320 6900 I www.amep.pr.gov.br

TIC do **STPP/RMC**;

Comunicar a importância de uma gestão eficaz da segurança da informação e da conformidade com os requisitos de gestão da segurança da informação;

Assegurar que a gestão de segurança da informação do **TIC** do **STPP/RMC** alcance os objetivos: Confidencialidade, Integridade e Disponibilidade.

4.2. DOS AGENTES DE TIC DO STPP/RMC

Cumprir a Política de Governança de Dados e Segurança e seus procedimentos correlatos;

Garantir que os colaboradores e fornecedores cumpram a **Política de Governança de Dados e Segurança do TIC do STPP/RMC**;

Implementar, controlar e manter ferramentas de controle e segurança do ambiente do **TIC** do **STPP/RMC**;

Implementar, controlar e manter ferramentas e controles para continuidade do serviço do **STPP/RMC** de acordo com o Plano de DRP: Plano de Recuperação de Tecnologia da Informação em Situações de Desastres.

5. PROCEDIMENTO

5.1. APRESENTAÇÃO

Este documento estabelece a Política de Governança de Dados e Segurança do **TIC do STPP/RMC**, um conjunto das diretrizes, normas e/ou procedimentos necessários à preservação e segurança das informações.

A Informação pode existir em muitas formas: pode ser impressa ou escrita em papel, guardada eletronicamente, transmitida pelo correio ou usando meios eletrônicos, mostrada em filmes, ou falada em conversação. Seja qual for a forma tomada pela Informação, meio através do qual ela é compartilhada ou armazenada, ela deve ser protegida adequadamente.

A Segurança da Informação é caracterizada pela preservação da Confidencialidade, Integridade, Disponibilidade.

AGÊNCIA DE ASSUNTOS METROPOLITANOS DO PARANÁ – AMEP
Palácio das Araucárias – Rua Jacy Loureiro de Campos, s/n – 1º andar – Centro Cívico – CEP 80.530-140 – Curitiba – Paraná
(41) 3320 6900 I www.amep.pr.gov.br

A Segurança da Informação é alcançada a partir da implementação de uma série de controles, que podem ser políticas, práticas, procedimentos, estruturas organizacionais, instalações, softwares e ferramentas de controle automatizadas. Estes controles devem ser estabelecidos para garantir que os objetivos de segurança do **STPP/RMC** sejam alcançados.

Abaixo alguns riscos típicos que esta Política pretende eliminar ou reduzir:

I. Revelação de Informações sensíveis;

II. Modificações indevidas ou perda de dados e programas;

III. Destruição ou perda de recursos computacionais e instalações;

IV. Interdições ou interrupções de serviços essenciais;

V. Roubo de propriedades, seja qual for.

As ameaças a serem tratadas por esta Política são:

I. Integridade: Prever ameaças de ambiente, externas ou internas, oriundas de catástrofes, fenômenos da natureza e/ou qualquer evento provocado intencionalmente ou não. Cita-se aqui, como exemplo, Ransomware, incêndio, pandemia, desastres, inundações entre outros.

II. Indisponibilidade: Prever falhas em sistemas e/ou diversos ambientes computacionais do **TIC do STPP/RMC.**

III. Divulgação da Informação: Prever a divulgação de Informações sensíveis aos **TIC do STPP/RMC**, premeditada e/ou acidental.

IV. Alterações não autorizadas: Prever alterações não autorizadas, premeditadas e/ou acidentais em Sistemas e/ou equipamentos de Tecnologia da Informação ou que suportem os processos do **STPP/RMC**.

As diretrizes que abrangem esta Política são:

I. Formalizar Procedimentos Gerenciais de Segurança da Informação, parte integrante desta Política, em conjunto com os Procedimentos Operacionais do

AGÊNCIA DE ASSUNTOS METROPOLITANOS DO PARANÁ – AMEP
Palácio das Araucárias – Rua Jacy Loureiro de Campos, s/n – 1º andar – Centro Cívico – CEP 80.530-140 – Curitiba – Paraná
(41) 3320 6900 I www.amep.pr.gov.br

TIC do STPP/RMC, compondo um conjunto de documentos eletrônicos, a serem mantidos e atualizados para consultas;

II. Divulgar a todos os **Agentes de TIC do STPP/RMC**, seus colaboradores, prestadores de serviços e/ou fornecedores, esta Política e suas responsabilidades pelo acesso ao **TIC** do **STPP/RMC**, evidenciando estas ações, no que lhe concerne;

III. Todos os agentes envolvidos no **TIC do STPP/RMC** assim como seus colaboradores, prestadores de serviços, fornecedores e terceiros, que de alguma forma possuírem acesso ao patrimônio de informações do **STPP/RMC**, são responsáveis pelo cumprimento desta Política.

5.2. DECLARAÇÃO DE COMPROMETIMENTO DOS AGENTES DE TIC DO STPP/RMC

Os Agentes de **TIC** do **STPP/RMC**, declaram-se comprometidos em proteger todos os ativos ligados à Tecnologia da Informação, garantindo a confidencialidade, a integridade e a disponibilidade de todos os ativos de informação. Para tanto, é enviada a todos os colaboradores, prestadores de serviços e fornecedores um termo de comprometimento com a **Política de Governança de Dados e Segurança**, bem como eventual Política de Segurança da Informação.

5.3. MONITORAMENTO

Para assegurar que o **Sistema de Gestão de Segurança da Informação** alcance seus resultados pretendidos serão realizadas auditorias de conformidade de acordo com a periodicidade definida pelo Poder Concedente.

5.4. ÁREAS DA SEGURANÇA A SEREM TRATADAS

5.4.1. SEGURANÇA FÍSICA

5.4.1.1. Conceituação

Conjunto de medidas destinadas à proteção e integridade dos ativos do **TIC do STPP/RMC** e à continuidade dos seus serviços.

AGÊNCIA DE ASSUNTOS METROPOLITANOS DO PARANÁ – AMEP
Palácio das Araucárias – Rua Jacy Loureiro de Campos, s/n – 1º andar – Centro Cívico – CEP 80.530-140 – Curitiba – Paraná
(41) 3320 6900 I www.amep.pr.gov.br

5.4.1.2. Vulnerabilidades

Devem ser previstos riscos naturais (inundações, tempestades entre outros), riscos acidentais (incêndios, interrupções de abastecimentos diversos entre outros), entradas não autorizadas, roubos de patrimônio, entre outros.

5.4.1.3. Áreas sensíveis

Devem ser mapeadas, levantadas e definida a criticidade de todos os ambientes físicos do **TIC do STPP/RMC**, principalmente os de alta criticidade, equipamentos, patrimônio físico, recursos humanos, entre outros. Devem ser contemplados acessos físicos a todos os ambientes e o monitoramento, principalmente os considerados de alta criticidade.

5.4.2. SEGURANCA LÓGICA

5.4.2.1. Conceituação

Conjunto de medidas destinadas à proteção de recursos computacionais contra utilização indevida ou desautorizada, intencional ou não.

5.4.2.2. Ambiente Lógico

O ambiente operacional, integrado pelos ativos de informação, de processamento e rede que deverá ser constantemente monitorado pelos **Agentes de TIC do STPP/RMC**.

5.4.2.3. Vulnerabilidades

Devem estar previstos acidentes por falhas e/ou sabotagem de hardware, software, aplicativos e procedimentos.

5.4.2.4. Áreas sensíveis

Sistemas Operacionais, Sistemas Gerenciais de Banco de Dados, Sistemas Gerenciais de Rede e ferramentas de apoio. Devem estar contempladas política de usuários e senhas com definição de perfis de acesso aos ambientes e aplicativos.

5.4.3. SEGURANCA DE TELECOMUNICACÃO

AGÊNCIA DE ASSUNTOS METROPOLITANOS DO PARANÁ – AMEP
Palácio das Araucárias – Rua Jacy Loureiro de Campos, s/n – 1º andar – Centro Cívico – CEP 80.530-140 – Curitiba – Paraná
(41) 3320 6900 I www.amep.pr.gov.br

5.4.3.1. Conceituação

Conjunto de medidas destinadas à proteção das Informações que trafegam por meios eletrônicos ou convencionais e dos recursos utilizados para esse tráfego.

5.4.3.2. Vulnerabilidades

Devem estar previstos acessos não autorizados às redes de comunicação de dados, adulteração de dados em tráfego, utilização não autorizada de informações, extravio de formulários ou documentos classificados para não disponibilização pública.

5.4.3.3. Áreas sensíveis

Redes de comunicação de dados, redes locais, conexões com redes externas, ligações de usuários externos aos servidores do **STPP/RMC**, telefonia.

5.4.4. CONTINUIDADE DO TIC DO STPP/RMC

5.4.4.1. Conceituação

Plano de Continuidade de Negócios (PCN) ou Conjunto de Planos que contemplam as atividades necessárias para a continuidade dos negócios, em conformidade com a ABNT NBR ISO 22.301, do **TIC do STPP/RMC**, quando houver algum tipo de interrupção nos processos, serviços e/ou equipamentos considerados críticos.

5.4.4.2. Vulnerabilidades

Devem estar previstas interrupções significativas das operações essenciais do **TIC do STPP/RMC**, causadas pelas vulnerabilidades nas áreas de segurança da informação a serem tratadas.

5.4.4.3. Áreas sensíveis

Todas as áreas de segurança da informação a serem tratadas.

5.4.5. Diretrizes

Para o perfeito funcionamento da **Política de Governança de Dados e Segurança do TIC do STPP/RMC**, as diretrizes a seguir devem ser implantadas e seguidas.

AGÊNCIA DE ASSUNTOS METROPOLITANOS DO PARANÁ – AMEP
Palácio das Araucárias – Rua Jacy Loureiro de Campos, s/n – 1º andar – Centro Cívico – CEP 80.530-140 – Curitiba – Paraná
(41) 3320 6900 I www.amep.pr.gov.br

5.4.5.1. Classificação e controle dos ativos

Os ativos devem ser gerenciados conforme o **Procedimento de Gestão de Ativos**

5.4.5.2. Incidentes de Segurança da Informação.

Entende-se como incidente de Segurança, qualquer evento em curso ou ocorrido que contrarie a política de segurança, comprometa a operação do **STPP** ou cause danos aos ativos.

Esse aspecto deve ser gerenciado de acordo com o **Procedimento de Incidentes de Segurança da Informação,** desta Política.

5.4.5.3. Gestão de Pessoas

Todas as pessoas envolvidas no **TIC do STPP/RMC** devem passar por treinamento nos procedimentos de Segurança da Informação e devem ser gerenciados acessos aos ativos desde a seleção até o desligamento.

5.4.5.4. Propriedade dos softwares aplicativos

Os sistemas aplicativos e/ou qualquer outro tipo de software, desenvolvidos ou adquiridos para o **TIC do STPP/RMC** devem ficar restritos ao sistema, não sendo permitida sua utilização para fins particulares e/ou cópias.

Esse aspecto deve ser gerenciado de acordo com o **Procedimento de Acesso a Recursos.**

5.4.5.5. Segurança Física

5.4.5.5.1. Área de Segurança

Os **Agentes de TIC do STPP/RMC** devem possuir estabelecido seu perímetro físico, identificando todas as suas "fronteiras" e identificando todos os pontos de acesso.

Para os acessos devem ser estabelecidos os controles necessários e suficientes, que salvaguardem as instalações dos **Agentes de TIC do STPP/RMC**.

Cabe a cada **Agente de TIC do STPP/RMC** definir, implementar e manter documentados os controles de acesso físico apropriados para proteger suas instalações, ativos de informação e recursos contra acesso não autorizado, danos e interferências.

AGÊNCIA DE ASSUNTOS METROPOLITANOS DO PARANÁ – AMEP
Palácio das Araucárias – Rua Jacy Loureiro de Campos, s/n – 1º andar – Centro Cívico – CEP 80.530-140 – Curitiba – Paraná
(41) 3320 6900 I www.amep.pr.gov.br

Estes controles devem ser baseados em uma análise de riscos periódica, considerando a criticidade das áreas e dos ativos a serem protegidos. Cada agente é responsável por estabelecer seus próprios procedimentos para a gestão de perímetros de segurança, controle de entradas físicas e monitoramento do ambiente.

5.4.5.5.2. Controles de Entrada e Saída de Pessoas

Os **Agentes de TIC do STPP/RMC** devem gerenciar o controle de entrada e saída de pessoas conforme o **Procedimento de Controle de Acesso Físico.**

5.4.5.6. Segurança Lógica

5.4.5.6.1. Gerenciamento das Operações e Comunicações

I. Documentação dos Procedimentos de Operação

Todos os sistemas, sejam eles executados em batch, on-line e/ou misto, estando em Produção, devem possuir documentação atualizada, conforme padrões de desenvolvimento seguro.

II. Ambiente Operacional

Todos os equipamentos de infraestrutura, interligações das redes, interligações de hardware de grande porte e softwares básicos e de apoio, devem possuir documentação necessária e suficiente, bem como atualizada, que possibilite entendimento a qualquer técnico capacitado e habilitado, visando manutenções preventivas, corretivas e evolutivas, no ambiente operacional.

III. Gerenciamento e controle de mudança

Toda e qualquer mudança no ambiente do **TIC do STPP/RMC**, seja ela de infraestrutura, hardware, comunicações, softwares básicos, softwares de apoio, sistemas aplicativos, procedimentos entre outros, deve ser executada conforme Procedimento de Gestão de Mudanças.

IV. Gerenciamento e controle de problemas

AGÊNCIA DE ASSUNTOS METROPOLITANOS DO PARANÁ – AMEP
Palácio das Araucárias – Rua Jacy Loureiro de Campos, s/n – 1º andar – Centro Cívico – CEP 80.530-140 – Curitiba – Paraná
(41) 3320 6900 I www.amep.pr.gov.br

Quaisquer problemas que ocorram no ambiente do **TIC do STPP/RMC**, sejam eles de infraestrutura, hardware, equipamentos de comunicação de dados, softwares e sistemas aplicativos, devem ser registrados com no mínimo, as seguintes Informações:

a) descrição do problema;

b) data e hora da ocorrência;

c) identificação de quem o registrou e quem foi acionado para solucioná-lo;

d) consequências do problema;

e) data e hora da solução;

f) identificação de quem solucionou;

g) descrição da solução adotada.

V. Monitoramento da Segurança

Testes periódicos de vulnerabilidade do ambiente de sustentação e operação do **TIC do STPP/RMC** deverão ser realizados com a finalidade de garantir que a implementação de segurança da informação está vigiada e monitorada de forma proativa.

VI. Incidentes de Segurança da Informação

Ocorrendo qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança lógica ou física dos ativos do **TIC do STPP/RMC** os mesmos deverão ser tratados conforme descrito no Procedimento de Incidentes de Segurança de Segurança da Informação.

VII. Comitê de Segurança da Informação (CSI)

Os Agentes de **TIC do STPP/RMC** deverão participar de grupo de gestão multidisciplinar, a ser instituído pelo **PODER CONCEDENTE**, que agrega várias visões corporativas às soluções de segurança, conhecido como comitê de segurança da informação.

As principais atribuições do Comitê de Segurança da Informação:

a) Revisar as Normas, Procedimentos e/ou Instruções de trabalho;

b) Avaliar direcionamento tecnológico para garantir segurança;

AGÊNCIA DE ASSUNTOS METROPOLITANOS DO PARANÁ – AMEP
Palácio das Araucárias – Rua Jacy Loureiro de Campos, s/n – 1º andar – Centro Cívico – CEP 80.530-140 – Curitiba – Paraná
(41) 3320 6900 I www.amep.pr.gov.br

c) Definir as atribuições pela Segurança da Informação ou do Grupo de Respostas a Incidentes de Segurança da Informação;

d) Aprovar as iniciativas para melhoria contínua das medidas de proteção dos bens de informação do **TIC do STPP/RMC**;

Este Comitê deve se reunir quando convocado pelo seu representante, ordinariamente e extraordinariamente, quando houver necessidade. As reuniões devem possuir como objetivo a avaliação e o aprimoramento da Política de Governança de Dados e Segurança, a análise das não-conformidades de Segurança e as ações adotadas para a correção e deverão ser registradas por Atas.

VIII. Grupo de resposta a incidentes (GRlSl).

Os **Agentes de TIC do STPP/RMC** devem estabelecer um grupo de pessoas que responderão pelos incidentes de segurança da informação nos ativos, visando documentar e conduzir as ações de resposta a estes incidentes, de forma organizada e controlada, que deve atuar junto a todo o parque tecnológico, inclusive pontos remotos.

IX. Prevenção, Detecção e Correção de Softwares Maliciosos

Medidas para prevenção, detecção e correção de Softwares Maliciosos deverão estar implementadas por todos os **Agentes de TIC do STPP/RMC**, para garantir a proteção dos ativos de informação contra softwares maliciosos.

X. Segurança de Redes

Assegurar que técnicas e procedimentos de segurança sejam usados para autorizar acessos e controlar as informações que circulam de e para as redes do **TIC do STPP/RMC**.

5.4.5.6.2. Procedimentos Operacionais

I. Política de backup

Os **Agentes de TIC do STPP/RMC** devem implementar o processo de Backup conforme Procedimento de Backup.

AGÊNCIA DE ASSUNTOS METROPOLITANOS DO PARANÁ – AMEP
Palácio das Araucárias – Rua Jacy Loureiro de Campos, s/n – 1º andar – Centro Cívico – CEP 80.530-140 – Curitiba – Paraná
(41) 3320 6900 I www.amep.pr.gov.br

II. Registros de Operações

Os **Agentes de TIC do STPP/RMC** devem implementar o processo de Registros de Operações conforme Procedimento de Registro de Operações.

5.4.5.6.3. Segurança e Tratamento de Mídias

Os **Agentes de TIC do STPP/RMC** devem definir e implementar um processo documentado para o manuseio seguro de todas as mídias (físicas ou eletrônicas) que contenham informações do **TIC do STPP/RMC**. Este processo deve abranger todo o ciclo de vida da mídia, incluindo o armazenamento, o transporte e o descarte seguro, garantindo a proteção das informações contra acesso não autorizado, perda ou roubo.

5.4.5.6.4. Controle de Acesso aos Recursos Computacionais

Os **Agentes de TIC do STPP/RMC** devem realizar o controle dos acessos conforme exposto nos Procedimentos de Classificação da Informação, de Senhas, e de Acesso a Recursos.

I. Identificação e autenticação de usuários

a) O usuário somente deve possuir acesso ao ambiente computacional através de uma identificação de acesso e uma senha;
b) A identificação de acesso do usuário deve ser única, pessoal e intransferível;
c) A senha associada à identificação de acesso deve ser secreta e de conhecimento exclusivo do usuário para o qual foi custodiada;
d) A senha não pode ser divulgada a terceiros, devendo-se evitar o uso de combinação simples ou óbvia na sua criação.

II. Uso das Estações de Trabalho

Os recursos computacionais, colocados à disposição dos **Agentes de TIC do STPP/RMC** deverão estar inventariados e o respectivo Termo de Responsabilidade assinado. Todo agente responde pelo mau uso ou dano causado nos equipamentos.

III. Arquivos Multimídias

AGÊNCIA DE ASSUNTOS METROPOLITANOS DO PARANÁ – AMEP
Palácio das Araucárias – Rua Jacy Loureiro de Campos, s/n – 1º andar – Centro Cívico – CEP 80.530-140 – Curitiba – Paraná
(41) 3320 6900 I www.amep.pr.gov.br

De maneira geral o uso de mídias e portas USB é proibido no ambiente do **TIC do STPP/RMC**. Liberações podem existir de acordo com a necessidade e avaliação de pessoas responsáveis.

Os agentes autorizados a utilizar mídias e portas USB devem assumir a responsabilidade de utilizar os acessos de forma ética e apenas para o exercício da função. Eles devem assinar o termo de responsabilidade.

5.4.5.6.5. Regras para criação de logins e senhas

Os **Agentes de TIC do STPP/RMC** devem garantir credenciais individuais. O compartilhamento de senhas é terminantemente proibido, pois expõe os agentes à responsabilidade pelas ações que outras pessoas realizarão com sua senha de acesso. Caso ocorra tal compartilhamento, seja de natureza autorizada ou não, os agentes serão responsabilizados pelas consequências das ações realizadas.

5.4.5.6.6. Perfil de acesso dos usuários

a) Cada usuário deve possuir um perfil de acesso à rede de dados que deve indicar os diretórios, grupos, aplicativos, funcionalidades e suas permissões de direito;
b) Aos sistemas, cada usuário deve possuir os perfis necessários para o desempenho de suas funções;
c) Sempre que necessário, deve ser estabelecido o mesmo perfil de acesso para um grupo de usuários;
d) Estes perfis devem estar normatizados;
e) A permissão de acesso aos ativos de informação do **TIC do STPP/RMC** deve ser solicitada formalmente conforme procedimento para liberação de acesso lógico.

5.4.5.6.7. Responsabilidades

As responsabilidades referentes ao controle de acesso aos recursos computacionais são classificadas conforme descrição abaixo:

I. Proprietário das Informações

AGÊNCIA DE ASSUNTOS METROPOLITANOS DO PARANÁ – AMEP
Palácio das Araucárias – Rua Jacy Loureiro de Campos, s/n – 1º andar – Centro Cívico – CEP 80.530-140 – Curitiba – Paraná
(41) 3320 6900 I www.amep.pr.gov.br

Pessoa que utiliza os recursos de Tecnologia da Informação de propriedade ou sobre custódia do **TIC do STPP/RMC** para a geração de informação de qualquer natureza.

Autoridade e a responsabilidade do proprietário das Informações:

a) Delegar responsabilidade e atribuições ao depositário das Informações;
b) Classificar os bens de Informação, de acordo com sua natureza crítica e sigilosa;
c) Estabelecer as regras de proteção dos bens de Informação, quanto aos acessos, backups entre outros;
d) Monitorar o cumprimento das regras estabelecidas;
e) Responder pelas violações registradas e participar da decisão a ser tomada, quando da ocorrência de não-conformidade;
f) Notificar não-conformidades de Segurança.

II. Custodiante

A Gestão de Tecnologia da Informação é a responsável pelo processamento, armazenamento e custódia das Informações.

Autoridade e responsabilidade do(a) Custodiante:

a) Administrar os controles estabelecidos pelo proprietário da aplicação e de seus dados;
b) Administrar o acesso aos recursos do sistema de processamento e prover procedimentos de Segurança;
c) Controlar o acesso à Informação;
d) Providenciar a proteção física;
e) Simular e executar os planos de continuidade;
f) Resolver as não-conformidades de Segurança.

III. Usuário da Informação

É todo colaborador, prestador de serviço, terceirizado, parceiro, estagiário ou fornecedor, que tenha acesso aos bens de Informação do **TIC do STPP/RMC**.

É vedada a utilização pelos Usuários da Informação dos recursos tecnológicos do **TIC do STPP/RMC** para fins pessoais.

AGÊNCIA DE ASSUNTOS METROPOLITANOS DO PARANÁ – AMEP
Palácio das Araucárias – Rua Jacy Loureiro de Campos, s/n – 1º andar – Centro Cívico – CEP 80.530-140 – Curitiba – Paraná
(41) 3320 6900 I www.amep.pr.gov.br

Autoridade e responsabilidade do usuário da Informação:

a) Zelar por todo acesso ao ambiente computadorizado executado e registrado com a sua identificação pessoal de acesso;
b) Respeitar e preservar o grau de confidencialidade da Informação, divulgando-a exclusivamente para os agentes autorizados a terem esse conhecimento;
c) Utilizar os recursos tecnológicos (equipamento, programas e sistemas) e as Informações somente para desempenho das suas atividades profissionais e dentro dos padrões de utilização descritos na Política de Governança de Dados e Segurança, sendo assim vedado o seu uso para fins pessoais;
d) Assinar o Termo de Responsabilidade e Sigilo onde são estabelecidas as regras sobre o uso dos bens de Informação;
e) Assinar o Termo de Responsabilidade e Compromisso, quando necessário, para utilização de funcionalidades que estejam fora dos padrões pré-determinados na Política de Governança de Dados e Segurança;
f) Notificar de imediato as não-conformidades de Segurança.

IV. Gestor do TIC do STPP/RMC

a) Gerenciar o cumprimento da Política de Governança de Dados e Segurança, por parte dos **Agentes de TIC do STPP/RMC**;
b) Identificar e comunicar a quem de direito os desvios praticados e adotar as medidas corretivas apropriadas;
c) Proteger, em nível físico e lógico, os ativos de informação sob sua responsabilidade;
d) Garantir que os **Agentes de TIC do STPP/RMC** compreendam e desempenhem a obrigação de proteger a informação do **TIC do STPP/RMC**.

V. Dos Agentes de TIC do STPP/RMC:

a) Cumprir integralmente a Política de Governança de Dados e Segurança, sob pena de incorrer nas sanções disciplinares e legais cabíveis;

AGÊNCIA DE ASSUNTOS METROPOLITANOS DO PARANÁ – AMEP
Palácio das Araucárias – Rua Jacy Loureiro de Campos, s/n – 1º andar – Centro Cívico – CEP 80.530-140 – Curitiba – Paraná
(41) 3320 6900 I www.amep.pr.gov.br

b) Preservar a integridade e guardar sigilo das informações de que fazem uso, bem como zelar e proteger os respectivos recursos de processamento de informações;
c) Utilizar os Sistemas de Informações e os recursos a ela relacionados somente para a execução das atividades correlacionadas com o desempenho do **TIC do STPP/RMC**;
d) Cumprir as regras específicas de proteção estabelecidas aos ativos de informação;
e) Manter o caráter sigiloso da senha de acesso aos recursos e sistemas do **TIC do STPP/RMC**;
f) Não compartilhar, sob qualquer forma, informações sigilosas com outros que não tenham a devida autorização de acesso;
g) Responder, por todo e qualquer acesso, aos recursos do **TIC do STPP/RMC**, bem como pelos efeitos desses acessos efetivados através do seu código de identificação, ou outro atributo para esse fim utilizado;
h) Respeitar a proibição de não usar, inspecionar, copiar ou armazenar programas de computador ou qualquer outro material, em violação da legislação de propriedade intelectual pertinente;
i) Comunicar ao gestor do **TIC do STPP/RMC** o conhecimento de qualquer irregularidade ou desvio da Política de Governança de Dados e Segurança.

5.4.5.6.8. Camadas de Segurança

Para a devida proteção do ambiente, devem ser projetadas 4 (quatro) camadas de acesso:

a) Acesso ao ambiente;
b) Acesso aos sistemas aplicativos;
c) Acesso às funções dos sistemas aplicativos;
d) Acesso aos dados.

Login e a senha de acesso devem ser únicos para todas as camadas de Segurança.

Devem ser exibidos para os usuários apenas os arquivos, os softwares e as funcionalidades a que eles têm direito de acesso.

5.4.5.6.9. Trilhas de Auditoria

AGÊNCIA DE ASSUNTOS METROPOLITANOS DO PARANÁ – AMEP
Palácio das Araucárias – Rua Jacy Loureiro de Campos, s/n – 1º andar – Centro Cívico – CEP 80.530-140 – Curitiba – Paraná
(41) 3320 6900 I www.amep.pr.gov.br

Devem existir softwares de Segurança que mantenham registros sobre os acessos dos usuários, indicando, sempre que possível, o arquivo, o software, a data e hora que foram acessados.

5.4.5.6.10. Computação Móvel e Trabalho Remoto.

Os **Agentes de TIC do STPP/RMC** devem gerenciar os ativos móveis e os acessos remotos para que estes sejam realizados com segurança. Devem ser previstos e adotados mecanismos visando a proteção dos bens de Informação, tais como Certificação digital, Softwares de Segurança, Antivírus, Firewalls corporativos e individuais, Criptografia e entre outros.

Deve ser vedado aos **Agentes de TIC do STPP/RMC** e seus colaboradores, prestadores de serviços, terceiros ou fornecedores, acesso ao ambiente do **TIC do STPP/RMC** com equipamentos de computação pessoal, salvo com autorização formal do gestor.

5.4.5.6.11. Trânsito de Informações

Os **Agentes de TIC do STPP/RMC** devem gerenciar o trânsito de informações conforme os Procedimentos de Classificação da Informação, de Acesso a Recursos e de Registro de Operações.

O trânsito de Informações deve ser feito por um caminho ou meio confiável com controles que ofereçam autenticidade do conteúdo, proteção de submissão, recebimento e não repúdio da origem. Os procedimentos acima citados contemplam e padronizam a geração, mudança, revogação, destruição, distribuição, certificação, armazenamento, entrada, uso e arquivamento de chaves criptográficas para garantir a proteção das informações contra modificação e acessos não autorizados.

5.4.5.6.12. Acesso a Utilitários Poderosos

Os **Agentes de TIC do STPP/RMC**, pela natureza dos serviços prestados e dos produtos comercializados relacionados à Segurança da Informação, devem gerenciar o uso de programas considerados poderosos, ou seja, programas que podem sobrepor os controles de Segurança estabelecidos e implementados.

AGÊNCIA DE ASSUNTOS METROPOLITANOS DO PARANÁ – AMEP
Palácio das Araucárias – Rua Jacy Loureiro de Campos, s/n – 1º andar – Centro Cívico – CEP 80.530-140 – Curitiba – Paraná
(41) 3320 6900 I www.amep.pr.gov.br

Estes utilitários possuem critérios de proteção de acesso que os tornam de uso restrito.

5.4.5.6.13. Administração de Acessos

Os **Agentes de TIC do STPP/RMC** devem gerenciar o acesso conforme os Procedimento de Classificação da Informação, Procedimento de Acesso a Recursos, Procedimento de Registro de Operações e Procedimento de Controle de Acesso Físico.

Os **Agentes de TIC do STPP/RMC** devem administrar e monitorar continuamente o acesso aos recursos computacionais, em conformidade com os princípios de controle de acesso e as diretrizes de geração e monitoramento de logs definidos nesta política, a fim de detectar e responder a atividades não autorizadas ou suspeitas.

O uso de contas e ferramentas com privilégios de administração (por exemplo: administrador de sistema, de banco de dados, dentre outros) representa um risco elevado e deve ser rigorosamente controlado. Cada **Agentes de TIC do STPP/RMC** deve implementar um processo para gerenciar o acesso privilegiado, que deve, no mínimo:

a) **Restringir o Acesso:** Limitar o número de usuários com acesso privilegiado ao mínimo estritamente necessário para a execução de suas funções.
b) **Exigir Aprovação Formal:** Conceder acesso privilegiado apenas mediante solicitação formal, justificativa e aprovação de um gestor responsável.
c) **Utilizar Credenciais Específicas:** Sempre que possível, o acesso privilegiado deve ser realizado com credenciais (usuário e senha) exclusivas para essa finalidade, distintas das credenciais de uso padrão do colaborador.
d) **Monitorar e Registrar o Uso:** Todas as atividades realizadas com credenciais privilegiadas devem ser registradas em logs detalhados. Esses logs devem ser protegidos contra adulteração e revisados periodicamente em busca de atividades suspeitas.

Devem ser realizados o monitoramento e gerenciamento dos acessos, pela Gestão e por auditores que porventura sejam requisitados.

5.4.5.6.14. Segurança no Ciclo de Vida de Desenvolvimento de Software (SDLC)

AGÊNCIA DE ASSUNTOS METROPOLITANOS DO PARANÁ – AMEP
Palácio das Araucárias – Rua Jacy Loureiro de Campos, s/n – 1º andar – Centro Cívico – CEP 80.530-140 – Curitiba – Paraná
(41) 3320 6900 I www.amep.pr.gov.br

A segurança da informação deve ser um componente integral de todo o processo de desenvolvimento e manutenção de sistemas do **TIC do STPP/RMC**. Os agentes devem adotar práticas de desenvolvimento seguro (DevSecOps), garantindo que, no mínimo, as seguintes atividades sejam contempladas:

a) **Requisitos de Segurança:** A definição de requisitos de segurança deve fazer parte da fase de planejamento de novas aplicações ou de alterações significativas.
b) **Codificação Segura:** Os desenvolvedores devem ser orientados a seguir práticas de codificação segura (secure coding), baseadas em padrões de mercado como o OWASP Top 10, para evitar vulnerabilidades comuns.
c) **Análise de Componentes de Terceiros:** As bibliotecas e componentes de código aberto ou de terceiros devem ser analisados para identificar e mitigar vulnerabilidades conhecidas (Análise de Composição de Software - SCA).
d) **Testes de Segurança:** Antes da entrada em produção, as aplicações devem ser submetidas a testes de segurança, que podem incluir Análise Estática (SAST), Análise Dinâmica (DAST) e/ou Testes de Invasão (Pen Tests), conforme a criticidade da aplicação.
e) **Gestão de Vulnerabilidades:** Deve existir um processo para tratar e corrigir as vulnerabilidades identificadas durante os testes e ao longo da vida útil da aplicação.

O desenvolvimento de sistema, seja ele feito pelos **Agentes de TIC do STPP/RMC** ou por empresas terceirizadas e/ou fornecedores, deve se atentar a metodologias com boas práticas e desenvolvimento seguro.

5.4.5.6.15. Segurança de Telecom

Os **Agentes de TIC do STPP/RMC** devem gerenciar a Segurança de Telecom conforme Procedimento de Acesso a Recursos.

5.4.5.6.16. Política de Uso Aceitável dos Recursos de Comunicação

Os **Agentes de TIC do STPP/RMC** devem definir, documentar, implementar e

comunicar a todos os seus usuários uma Política de Uso Aceitável (PUA) que rege o uso de todos os recursos de comunicação eletrônica, incluindo acesso à internet, e-mail, mensagens instantâneas e outras plataformas.

A PUA de cada agente deve estabelecer que os recursos são fornecidos para fins profissionais e devem ser utilizados de forma ética, legal e segura. A política deve abordar, no mínimo, os seguintes princípios:

a) **Uso Profissional e Monitoramento:** O uso dos recursos é primariamente para atividades de negócio. A política deve definir os limites para um eventual uso pessoal incidental e informar aos usuários que o uso dos recursos pode ser monitorado, em conformidade com a legislação vigente.

b) **Proteção da Informação Confidencial:** É estritamente proibido o compartilhamento de informações confidenciais ou restritas do **TIC do STPP/RMC** em qualquer fórum público, rede social, grupo de discussão ou através de canais de comunicação não seguros. A política deve orientar os usuários a utilizar canais e métodos seguros (como criptografia) para a transmissão de dados sensíveis, quando autorizados.

c) **Conteúdo Inapropriado:** É proibida a criação, o armazenamento ou a divulgação de qualquer conteúdo que seja ilegal, malicioso, ofensivo, discriminatório, pornográfico ou que possa causar dano à reputação do **TIC do STPP/RMC** ou de seus agentes.

d) **Controles de Segurança:** O agente deve implementar controles técnicos para proteger sua rede e reforçar esta política. Isso inclui o uso de firewalls, sistemas de filtragem de conteúdo web e proteção contra software malicioso (malware) no tráfego de internet e e-mail. A tentativa de contornar esses controles de segurança é estritamente proibida.

5.4.5.7. Condutas Gerais

As Políticas de conduta gerais abordadas abaixo, devem ser implementadas pelos **Agentes de TIC do STPP/RMC**.

AGÊNCIA DE ASSUNTOS METROPOLITANOS DO PARANÁ – AMEP
Palácio das Araucárias – Rua Jacy Loureiro de Campos, s/n – 1º andar – Centro Cívico – CEP 80.530-140 – Curitiba – Paraná
(41) 3320 6900 I www.amep.pr.gov.br

5.4.5.7.1. Política de mesa e tela limpas

I. Mesa Limpa

a) Os documentos em papéis e mídias eletrônicas não devem permanecer sobre a mesa desnecessariamente, devem ser armazenados em armários ou gavetas trancados, quando não estiverem em uso, especialmente fora do horário do expediente;
b) Não anotar informações sensíveis em quadros brancos ou Post-it;
c) Guardar agendas e cadernos de anotações numa gaveta trancada;
d) Manter os pertences pessoais em gavetas ou armários trancados,
e) Manter as gavetas e armários fechados e trancados, não deixar as chaves na fechadura, não deixar chaves em qualquer lugar as mantenha junto a você;
f) Nunca escrever senhas em lembretes e nem tente escondê-las no local de trabalho;
g) Não deixe mídias nos drives;
h) Ao final do expediente, ou no caso de ausência prolongada do local de trabalho, limpar a mesa de trabalho, guardar os documentos, trancar as gavetas e armários, e desligar computador;
i) Não colocar ou comer refeições e lanches sobre a mesa;
j) Trancar o local de trabalho ao deixá-lo, não deixar o local de trabalho aberto sem que haja um colaborador que trabalhe no local presente.

II. Tela Limpa

a) Computadores pessoais, terminais de computador e impressoras não devem ser deixados "logados", caso o usuário responsável não esteja presente, com bloqueio automático via GPO;
b) Celulares corporativos devem conter tela de bloqueio para restringir acesso de terceiro a dados dos clientes que por ventura possam circular pelo aparelho;

AGÊNCIA DE ASSUNTOS METROPOLITANOS DO PARANÁ – AMEP
Palácio das Araucárias – Rua Jacy Loureiro de Campos, s/n – 1º andar – Centro Cívico – CEP 80.530-140 – Curitiba – Paraná
(41) 3320 6900 I www.amep.pr.gov.br

c) Nos computadores, utilizar um protetor de tela que solicite uma senha para acesso.

5.4.5.7.2. Documentação física

I. Armazenamento seguro

As informações críticas devem ser guardadas em lugar seguro quando não em uso, principalmente quando o escritório está desocupado.

II. Cuidados com impressão

Dentro das possibilidades não devem ser impressos nenhum documento. Caso seja necessários impressão, documentos com informações sensíveis devem ser recolhidos imediatamente, a fim de impedir que uma pessoa não autorizada tenha acesso à informação.

Pontos de entrada e saída de correspondência devem ser protegidos e monitorados.

III. Cuidados com o Lixo

Todo lixo que contenha informação reservada ou secreta deve ser eliminado através de "Máquina picotadora" ou similar, ou destruição manual. Sempre se certifique que o descarte ocorreu de maneira correta e que impossibilita qualquer tentativa de reconstrução.

5.4.5.7.3. Conduta em ambiente externo:

a) É fundamental que os **Agentes de TIC do STPP/RMC** sejam reservados e cuidadosos nas suas opiniões, conversas, participações em eventos, principalmente quando em contato com o cliente e/ou com terceiros;
b) Cuidado com as informações sensíveis e com as conversas em locais públicos, aplicativos e meios de transporte.

5.4.5.8. Gestão de Fornecedores

Os **Agentes de TIC do STPP/RMC** devem realizar o gerenciamento dos fornecedores e terceiros que operam informações, sistemas e ferramentas relativos ao **TIC do**

STPP/RMC. Devem ser implementadas regras de diligência adicionais para terceiros considerados relevantes, que são aqueles que são considerados críticos a operação.
Devem ser avaliados e homologados os fornecedores críticos, através de critérios de avaliação para classificar o nível de aderência em Segurança da Informação.

5.4.5.9. Sanções

A não observância dos dispositivos desta Política sujeita os infratores, isolada ou cumulativamente, a sanções administrativas, trabalhistas cíveis e penais previstas em legislação e em regulamentação vigentes, assegurados aos envolvidos o direito ao contraditório e à ampla defesa.

AGÊNCIA DE ASSUNTOS METROPOLITANOS DO PARANÁ – AMEP
Palácio das Araucárias – Rua Jacy Loureiro de Campos, s/n – 1º andar – Centro Cívico – CEP 80.530-140 – Curitiba – Paraná
(41) 3320 6900 I www.amep.pr.gov.br

PLANO DE DRP: PLANO DE RECUPERAÇÃO DE TECNOLOGIA DA INFORMAÇÃO EM SITUAÇÕES DE DESASTRES

1. OBJETIVO

O objetivo do Plano de Recuperação de Desastres (DRP) é diminuir ao máximo o downtime, ou tempo de indisponibilidade, das operações e reduzir ao máximo a perda dos dados. Para atingir objetivos o DRP deve atender os seguintes requisitos.

Reduzir as perdas financeiras em casos de desastres e minimizar a duração de uma paralisação das operações do **TIC do STPP/RMC**.

2. RESPONSABILIDADES

2.1. GESTOR DO TIC DO STPP/RMC

I. Avaliar os impactos de potenciais riscos ao processo;

II. Aprovar os documentos e procedimentos para continuidade do **TIC do STPP/RMC**;

III. Garantir a ciência de todos os colaboradores sobre a priorização a ser seguida na preservação dos recursos do **TIC do STPP/RMC**;

IV. Tomar decisões sobre a necessidade de ações durante as crises, no caso de acionamento do Plano de D&R;

V. Comunicar seus agentes sobre eventuais crises;

VI. Comunicar seus colaboradores sobre eventuais crises;

VII. Comunicar DPO em caso de incidentes com impacto em dados de pessoa física;

VIII. Comunicar seus clientes sobre eventuais crises;

IX. Comunicar órgãos reguladores, se aplicável;

X. Comunicar mercado sobre eventuais crises;

XI. Definir padrões de criação, controle e divulgação dos documentos do **TIC do STPP/RMC** para elevar o nível de governança.

AGÊNCIA DE ASSUNTOS METROPOLITANOS DO PARANÁ – AMEP
Palácio das Araucárias – Rua Jacy Loureiro de Campos, s/n – 1º andar – Centro Cívico – CEP 80.530-140 – Curitiba – Paraná
(41) 3320 6900 I www.amep.pr.gov.br

2.2. COMITÊ DE CRISE

I. Avaliar riscos que possam recair sobre a categoria de crises, quando de seu acontecimento, a fim de prevenir, evitar, compartilhar ou aceitar riscos;

II. Informar os **Agentes de TIC do STPP/RMC** sobre as situações de crise e de acionamento do Plano de D&R para tomada de decisões;

III. Avaliar a necessidade de comunicação interna e externa de incidentes de SI, de acordo como a decisão do **Gestor do TIC do STPP/RMC**.

2.3. AGENTES DE TIC DO STPP/RMC

I. Comunicar imediatamente a iminência do acontecimento de uma crise, quando não for percebida pelos agentes anteriores;

II. Cumprir os planos de acordo com o que for estabelecido antes, durante a comunicação de crises;

III. Comunicar autoridades locais sempre que necessário (ex.: bombeiros, defesa civil, polícia etc.).

2.4. TECNOLOGIA DA INFORMAÇÃO (TI)

I. Observar e cumprir as diretrizes dispostas nesse plano de recuperação de desastres;

II. Promover as melhores práticas e disseminar as diretrizes deste Plano;

III. Dar tratamento adequado a todos os casos de não conformidade identificados ou que lhe forem reportados;

IV. Manter o Controle de Registros atualizado.

AGÊNCIA DE ASSUNTOS METROPOLITANOS DO PARANÁ – AMEP
Palácio das Araucárias – Rua Jacy Loureiro de Campos, s/n – 1º andar – Centro Cívico – CEP 80.530-140 – Curitiba – Paraná
(41) 3320 6900 I www.amep.pr.gov.br

3. COMUNICAÇÃO E RESPONSABILIDADES

3.1. RESPONSABILIDADES

Matriz de Responsabilidades D&R					
Cenário	**Acionamento do Plano de D&R**	**Informado internamente**	**Tomador de Decisão**	**Consultado**	**Informado externamente**
Ransomware	TI	Comitê de Crise, Agentes de TIC do STPP/RMC	Gestor do TIC do STPP/RMC	Gestor da T.I do Estado	Agentes de TIC do STPP/RMC, colaboradores, clientes, mídias, órgãos reguladores
Vazamento de Dados	TI	Comitê de Crise, Agentes de TIC do STPP/RMC	Gestor do TIC do STPP/RMC	Gestor da T.I do Estado	Agentes de TIC do STPP/RMC, colaboradores, clientes, mídias, órgãos reguladores
Abuso de Acesso Autorizado	TI	Comitê de Crise, Agentes de TIC do STPP/RMC	Gestor do TIC do STPP/RMC	Gestor da T.I do Estado	Agentes de TIC do STPP/RMC, colaboradores, clientes, mídias, órgãos reguladores
Crise Energética	TI	Comitê de Crise, Agentes de TIC do STPP/RMC	Gestor do TIC do STPP/RMC	Gestor da T.I do Estado	Agentes de TIC do STPP/RMC, colaboradores, clientes, mídias, órgãos reguladores
Crise Política	TI	Comitê de Crise, Agentes de TIC do STPP/RMC	Gestor do TIC do STPP/RMC	Gestor da T.I do Estado	Agentes de TIC do STPP/RMC, colaboradores, clientes, mídias, órgãos reguladores
Perda de Datacenter	TI	Comitê de Crise, Agentes de TIC do STPP/RMC	Gestor do TIC do STPP/RMC	Gestor da T.I do Estado	Agentes de TIC do STPP/RMC, colaboradores, clientes, mídias, órgãos reguladores
Falha de comunicação dos equipamentos embarcados	TI	Comitê de Crise, Agentes de TIC do STPP/RMC	Gestor do TIC do STPP/RMC	Gestor da T.I do Estado	Agentes de TIC do STPP/RMC, colaboradores, clientes, mídias, órgãos reguladores
Sucessão Planejada	TI	Comitê de Crise, Agentes de TIC do STPP/RMC	Gestor do TIC do STPP/RMC	Gestor da T.I do Estado	Agentes de TIC do STPP/RMC, colaboradores, clientes, mídias, órgãos reguladores
Terceirização	TI	Comitê de Crise, Agentes de TIC do STPP/RMC	Gestor do TIC do STPP/RMC	Gestor da T.I do Estado	Agentes de TIC do STPP/RMC, colaboradores, clientes, mídias, órgãos reguladores

3.2. COMUNICAÇÃO

A comunicação de situações de crise deve seguir o procedimento e fluxo abaixo:

AGÊNCIA DE ASSUNTOS METROPOLITANOS DO PARANÁ – AMEP
Palácio das Araucárias – Rua Jacy Loureiro de Campos, s/n – 1º andar – Centro Cívico – CEP 80.530-140 – Curitiba – Paraná
(41) 3320 6900 I www.amep.pr.gov.br

Mensagens Chave:

INFORMAÇÃO EXTERNA

Nossos sistemas estão sofrendo uma instabilidade temporária e estamos trabalhando para que sejam restabelecidos o mais breve possível.

O _***(Agente do TIC do STPP/RMC)***_ não medirá esforços para restabelecer a operação e assegurar que os dados de todos os públicos envolvidos sejam preservados.

INFORMAÇÃO INTERNA:

Nossos sistemas estão sofrendo uma instabilidade temporária, atribuída a um ataque cibernético e estamos trabalhando para que sejam restabelecidos o mais breve possível. Ainda não temos total visibilidade do ataque sofrido e da sua extensão. Todos os envolvidos já foram acionados e manteremos todos informados. Não mediremos esforços para restabelecer a operação e assegurar que os dados sejam preservados.

Matriz Stakeholders	Alto/ Baixo Impacto	Ação	O que fazer?	Porta-Voz
Clientes	Alto	Comunicação Canais Oficiais - Abertos	Comunicado via Site, Card WhatsApp para envio à equipe para distribuição, URA (mensagem automática).	Canais de Comunicação formais.
Comunidade (público geral - Usuários)	Alto	Comunicação Canais Oficiais - Abertos	Comunicado via Site, Card WhatsApp para envio à equipe para distribuição, URA (mensagem automática).	Canais de Comunicação formais.
Colaboradores: Alta Gestão (diretores)	Alto	Comunicação Canais Oficiais - Internos	Canal de Comunicação Interno, Grupos de WhatsApp Internos, Banner na Extranet (Caso não esteja comprometido), Vídeo (caso necessário).	
Colaboradores: Média Gestão (gerentes)	Alto			
Colaboradores: Operacional - Direto	Alto			
Colaboradores: Influenciadores	Alto			
Associados: operadoras de transporte	Alto	Comunicado Formal Direto - Diretoria	Comunicado Formal com assinatura do CEO	
Governo	Alto	Comunicado Formal Direto - DPO	Comunicado à ANPD.	
Terceiros	Alto	Comunicação Canais Oficiais - Abertos	Comunicado via Site, Card WhatsApp para envio à equipe para distribuição, URA (mensagem automática).	
Fornecedores	Alto			

AGÊNCIA DE ASSUNTOS METROPOLITANOS DO PARANÁ – AMEP
Palácio das Araucárias – Rua Jacy Loureiro de Campos, s/n – 1º andar – Centro Cívico – CEP 80.530-140 – Curitiba – Paraná
(41) 3320 6900 I www.amep.pr.gov.br

Entidades Financeiras	Alto	Comunicado Formal Direto - Diretoria	Comunicado Formal com assinatura do CEO	
Imprensa local	Alto	Comunicado Assessoria de Imprensa	Comunicado de Imprensa	
Imprensa regional, nacional	Alto		Comunicado de Imprensa	
Hackers	Alto	Digital	Negociação	Diretoria, Comitê Direto de Crise

4. CENÁRIOS DE DESASTRE

4.1. RANSOMWARE

4.1.1. DEFINIÇÃO

Ransomware é um tipo de malware de sequestro de dados, feito por meio de criptografia, que usa como refém arquivos pessoais da própria vítima ou dados da organização e cobra resgate para restabelecer o acesso a estes arquivos.

4.1.2. PROCEDIMENTO

4.1.2.1. IDENTIFICAÇÃO

Detectar que está em uma situação de crise, declarar o cenário de Ransomware e seguir para a contenção.

4.1.2.2. CONTENÇÃO

A atividade de contenção envolve isolar o problema o máximo possível, para que ele não afete outros serviços.

Dependendo da gravidade da crise ou ainda se não conseguir dimensionar a gravidade, desconectar o ambiente. Caso identificado que o cenário não é crítico, seguir com as ações seguintes:

I. Bloquear os IOC´s usando as ferramentas disponíveis (AV, Firewall etc.);

II. Bloquear as credenciais comprometidas;

III. Desabilitar todas as contas com privilégios;

IV. Desconectar os hosts comprometidos da rede:

V. Desligar todas as funcionalidades Wireless: Wi-Fi, Bluetooth, NFC;

AGÊNCIA DE ASSUNTOS METROPOLITANOS DO PARANÁ – AMEP
Palácio das Araucárias – Rua Jacy Loureiro de Campos, s/n – 1º andar – Centro Cívico – CEP 80.530-140 – Curitiba – Paraná
(41) 3320 6900 I www.amep.pr.gov.br

VI. Desconectar/Isolar pelo menos um controlador de domínio (ideal 2);

VII. Desconectar/Isolar servidores ainda não comprometidos;

VIII. Desativar o PowerShell em todas as máquinas (caso a solução de segurança AV suporte);

IX. Elaborar Check list para Tratamento de Incidente Ransomware.

4.1.2.3. ERRADICAÇÃO

A atividade de erradicação, envolve investigar e resolver o problema que gerou o incidente. A correta identificação e entendimento do incidente é fundamental para o sucesso dessa atividade.

Abrir um Registro do Incidente. O ideal é que esse Registro de Incidente seja compartilhado com todos que irão atuar ou atuaram no incidente. Todas as ações devem ser registradas no Registro de Incidente.

Entrevistar os envolvidos para um melhor entendimento do incidente, ações já realizadas, datas e horários, impacto ambiente até o momento.

Identificar os fatos do incidente:

X. Verificar sistemas de chamados em busca de relatos em que o usuário não consegue utilizar o sistema ou que arquivos mudaram de extensão (Mapear máquinas);

XI. Paciente Zero (Fonte da infecção) - Procurar no servidor de arquivos por usuário com centenas de arquivos abertos, provavelmente ele é a fonte da infecção;

XII. Verificar logs dos equipamentos de segurança. (Firewall, AV);

XIII. Identificar SO´s comprometidos;

XIV. Identificar o tipo, grupo hacker proprietário e versão do ransomware (se possível);

XV. Identificar os IOC´s (Identificadores de comprometimento como hashs de arquivos, e-mails phishing);

XVI. Identificar possíveis credenciais comprometidas;

XVII. Identificar aplicações comprometidas;

XVIII. Levantar aplicações críticas para o negócio;

AGÊNCIA DE ASSUNTOS METROPOLITANOS DO PARANÁ – AMEP
Palácio das Araucárias – Rua Jacy Loureiro de Campos, s/n – 1º andar – Centro Cívico – CEP 80.530-140 – Curitiba – Paraná
(41) 3320 6900 I www.amep.pr.gov.br

XIX. Enviar um arquivo exemplo do ransomware para análise. (VirusTotal / Fabricante AV);

XX. Elaborar Check list para Tratamento de Incidente Ransomware.

XXI. Remover o Ransomware dos sistemas infectados:

XXII. Fazer deploy de NGAV;

XXIII. Aplicar baseline de segurança;

4.1.2.4. RECUPERAÇÃO

A atividade de recuperação envolve voltar o ambiente ao status de totalmente operacional, sendo pela restauração de backups, pagamento pelo resgate dos dados ou pela reinstalação e reconfiguração do ambiente.

É muito importante que as seguintes etapas anteriores sejam completadas: contenção e a identificação da causa raiz e a data da infecção antes de iniciar o processo de recuperação.

Restauração de Backups:

I. Verificar existência de Shadow Copies;

II. Verificar se existem versões do backup em nuvem;

III. Se certificar de que todos os arquivos necessários estão disponíveis;

IV. Verificar a integridade do backup e fazer restauração dos dados;

V. Backup Imutável.

Tentar descriptografar:

I. Determinar tipo, fabricante e versão do ransomware (se possível);

II. Procurar um decryptor, caso encontre, tentar a descriptografia;

III. Negociar e pagar o resgate. Os principais motivos para se considerar o pagamento devem ser a perda potencial de vidas ou o potencial colapso para a empresa se as operações não forem restabelecidas imediatamente;

IV. Se possível negociar um valor menor ou parcelamento;

V. Entender quais métodos de pagamentos aceitos (Bitcoin, Cachcard);

VI. Conseguir o meio de pagamento (normalmente Bitcoin);

VII. Reconectar computadores encriptados na Internet;

AGÊNCIA DE ASSUNTOS METROPOLITANOS DO PARANÁ – AMEP
Palácio das Araucárias – Rua Jacy Loureiro de Campos, s/n – 1º andar – Centro Cívico – CEP 80.530-140 – Curitiba – Paraná
(41) 3320 6900 I www.amep.pr.gov.br

VIII. Instalar TOR Browser;

IX. Pegar o endereço da carteira de Bitcoin. Isso pode ser visto na tela do Ransomware ou no site TOR que foi criado pelo Ransomware;

X. Pagar o resgate. Transferir o valor para a carteira. Pagar um resgate não é igual a recuperação instantânea e pode ferir leis federais (Envolver time jurídico). Não há garantia de descriptografia mesmo após o pagamento;

XI. Averiguar se todos os itens que foram criptografados estão conectados ao computador. O retorno dos arquivos acontece em 24 horas, mas não é incomum começar antes;

XII. Reinstalar nas máquinas infectadas o NGAV (Antes de colocar a máquina na rede);

XIII. Instalar Siem (Antes de colocar a máquina na rede).

4.2. VAZAMENTO DE DADOS

4.2.1. DEFINIÇÃO

Vazamento de dados é um incidente de segurança que expõe publicamente informações sensíveis que podem ser vistas, copiadas, roubadas, transmitidas ou usadas sem acesso autorizado.

4.2.2. PROCEDIMENTO

4.2.2.1. IDENTIFICAÇÃO

A identificação de situação de vazamentos de dados pode se dar por qualquer Agente, colaborador do **TIC do STPP/RMC** ou através do cliente que sofreu danos com a situação.

4.2.2.2. CONTENÇÃO

Após a identificação do vazamento de dados é necessário o registro de Incidente de Segurança da Informação para que a ocorrência seja tratada. O registro deve ser realizado através de abertura de chamado de Incidente de Segurança.

O registro deve conter, no mínimo, os seguintes dados:

AGÊNCIA DE ASSUNTOS METROPOLITANOS DO PARANÁ – AMEP
Palácio das Araucárias – Rua Jacy Loureiro de Campos, s/n – 1º andar – Centro Cívico – CEP 80.530-140 – Curitiba – Paraná
(41) 3320 6900 I www.amep.pr.gov.br

I. Quais dados foram identificados que sofreram vazamento;

II. Onde os dados estão expostos;

III. Qual a exposição (tamanho da base que pode ter acesso aos dados vazados);

IV. Existência de legislação que incide sobre os dados vazados;

V. Necessidade de comunicação aos órgãos governamentais;

VI. Necessidade de comunicação às partes interessadas;

VII. Necessidade de comunicação à Comunidade.

Após a realização do registro, a equipe de TI deve entender a possibilidade de recuperar a informação vazada. Não havendo essa possibilidade, deve acionar a Gestão para identificar as ações de comunicação e de cumprimento de requisitos, sejam eles legais ou contratuais.

4.3. ABUSO DE ACESSO AUTORIZADO

4.3.1. DEFINIÇÃO

O acesso privilegiado se refere a contas com recursos elevados que vão além dos usuários normais.

Uma credencial é considerada como acesso privilegiado quando possui direitos para administrar outras contas; alterar, remover arquivos e programas; gerenciar contatos; conceder ou revogar o acesso de outros usuários a sistemas.

4.3.2. PROCEDIMENTO

4.3.2.1. IDENTIFICAÇÃO

Todos os usuários que possuem credenciais para acesso privilegiado devem possuir ferramenta de cofre de senhas, troca de senhas programadas e periódicas, e monitoramento de acesso.

4.3.2.2. CONTENÇÃO

São realizadas como ação preventiva revisões periódicas de acesso dos usuários, incluindo colaboradores, terceiros e fornecedores.

AGÊNCIA DE ASSUNTOS METROPOLITANOS DO PARANÁ – AMEP
Palácio das Araucárias – Rua Jacy Loureiro de Campos, s/n – 1º andar – Centro Cívico – CEP 80.530-140 – Curitiba – Paraná
(41) 3320 6900 I www.amep.pr.gov.br

Para acessos de fora da companhia deve ser utilizada VPN com aplicação de Multi Fator de Autenticação (MFA).

4.3.2.3. RECUPERAÇÃO

Se houver um ataque de Ransomware, deverá ser utilizado procedimento de recuperação de incidentes Ransomware.

4.4. CRISE ENERGÉTICA

4.4.1. DEFINIÇÃO

Momento em que a disponibilidade ou a entrega dentro da normalidade de energia é comprometida por diversas situações, por uma variedade de fatores, tanto previsíveis quanto imprevisíveis, exigindo medidas de racionamento ou resultando em falhas no sistema.

4.4.2. PROCEDIMENTO

4.4.2.1. IDENTIFICAÇÃO

A identificação do cenário se dá a partir do momento da falta de energia nas unidades do **TIC do STPP/RMC**, com acionamento à unidade responsável pela distribuição, para informação do tempo previsto da indisponibilidade. A partir dessa informação é tomada a decisão de acionamento do Plano de Contenção.

4.4.2.2. CONTENÇÃO

Para as funções administrativas serão acionados os geradores da unidade.
Para as funções operacionais serão realizadas as atividades que são possíveis com energia elétrica restrita, até o restabelecimento total.

4.4.2.2.1. Agentes de TIC do STPP/RMC

Em relação ao serviço prestados pelos **Agentes de TIC do STPP/RMC**, deve ser realizado o acionamento dos procedimentos de contingência estabelecido por cada Agente.

AGÊNCIA DE ASSUNTOS METROPOLITANOS DO PARANÁ – AMEP
Palácio das Araucárias – Rua Jacy Loureiro de Campos, s/n – 1º andar – Centro Cívico – CEP 80.530-140 – Curitiba – Paraná
(41) 3320 6900 I www.amep.pr.gov.br

4.4.2.3. RECUPERAÇÃO

A recuperação acontece após o restabelecimento da energia elétrica, retornando as atividades e restabelecendo as operações.

4.5. PERDA DE DATACENTER

4.5.1. DEFINIÇÃO

Local físico que armazena máquinas de computação e seus equipamentos de hardware relacionados. E contém a infraestrutura de computação que os sistemas de TI exigem, como servidores, unidades de armazenamento de dados e equipamentos de rede.
A perda de Datacenter pode se dar das seguintes formas:
Alagamento, incêndio, explosão, problemas de infraestrutura, falha de energia, Terremotos, intempéries, desastres em geral.

4.5.2. PROCEDIMENTO

4.5.2.1. IDENTIFICAÇÃO

A TI é responsável por realizar o monitoramento dos serviços e identificar se há alguma interrupção de serviço em algum dos datacenters, ou mesmo nos sites.

4.5.2.2. CONTENÇÃO

Após a identificação da indisponibilidade em algum dos sites, realizar a migração, caso necessário.
Para o caso de indisponibilidade nos Datacenters deve ser implementada a replicação dos serviços críticos e ainda ser criado um ambiente virtual para utilização do backup na retomada dos serviços.

4.5.2.3. ERRADICAÇÃO

O plano de ação para erradicação é migrar o datacenter redundante para a Nuvem.

4.5.2.4. RECUPERAÇÃO

AGÊNCIA DE ASSUNTOS METROPOLITANOS DO PARANÁ – AMEP
Palácio das Araucárias – Rua Jacy Loureiro de Campos, s/n – 1º andar – Centro Cívico – CEP 80.530-140 – Curitiba – Paraná
(41) 3320 6900 I www.amep.pr.gov.br

Após identificação do retorno à normalidade da disponibilidade dos serviços, retornar à situação de configuração.

4.6. FALHA DE COMUNICAÇÃO DOS EQUIPAMENTOS EMBARCADOS

4.6.1. DEFINIÇÃO

Equipamentos embarcados, também conhecidos como sistemas embarcados, são dispositivos dedicados a realizar funções específicas dentro de um sistema maior. São chamados de "embarcados" por serem integrados com outros dispositivos e/ou sistemas e geralmente não são projetados para serem utilizados de forma independente.

4.6.2. CONTEXTO

A perda dos sistemas embarcados pode se dar das seguintes formas: incêndio, problemas de alimentação elétrica, problemas de infraestrutura, furto, roubo, enchente.
No **SBE** (Sistema de Bilhetagem Eletrônica), por exemplo, os sistemas embarcados são:

I. Validador e seus componentes;
II. MITS.

4.6.3. PROCEDIMENTO

4.6.3.1. IDENTIFICAÇÃO

Recomenda-se que os sistemas embarcados sejam monitorados constantemente pela equipe de TI da Concessionária, e se necessário acionar o fornecedor responsável pela tecnologia.
Havendo alguma indisponibilidade o fornecedor responsável pela tecnologia deverá informar imediatamente a TI da Concessionária.

4.6.3.2. CONTENÇÃO

A contenção para a indisponibilidade do equipamento é a substituição direta dele por um idêntico.

4.6.3.3. ERRADICAÇÃO

AGÊNCIA DE ASSUNTOS METROPOLITANOS DO PARANÁ – AMEP
Palácio das Araucárias – Rua Jacy Loureiro de Campos, s/n – 1º andar – Centro Cívico – CEP 80.530-140 – Curitiba – Paraná
(41) 3320 6900 I www.amep.pr.gov.br

Deverão ser implementados controles para mitigar os impactos em caso de indisponibilidade tais como:

I. Datacenter redundante;
II. Backup;
III. Replicação dos serviços críticos em nuvem;
IV. Procedimentos de operação;
V. Gestão da Mudança.

4.6.3.4. RECUPERAÇÃO

A recuperação acontece quando o serviço é restabelecido.

4.7. DESASTRE

4.7.1. DEFINIÇÃO

Resultado de eventos adversos, naturais ou provocados pelo homem, sobre um ecossistema vulnerável, causando danos humanos, materiais e ambientais e consequentes prejuízos econômicos e sociais. Exemplos de desastres: alagamento, enchente, explosão, acidente aéreo, podendo ocorrer no **STPP** ou nas instalações que compõem **TIC do STPP/RMC**.

4.7.2. PROCEDIMENTO

4.7.2.1. IDENTIFICAÇÃO

Situações de desastre podem ser identificadas através do monitoramento nos canais de comunicação da Defesa Civil onde existe operação do **STPP**. Ainda pode ser possível a identificação de uma situação de desastre em qualquer um dos **Agentes de TIC do STPP/RMC** pelos colaboradores, parceiros de negócio e fornecedores ou ainda monitoramento dos serviços pela TI.

4.7.2.2. CONTENÇÃO

Após a identificação de um cenário de desastre podem ser possíveis as seguintes ações, a serem avaliadas as pertinências em cada caso:

AGÊNCIA DE ASSUNTOS METROPOLITANOS DO PARANÁ – AMEP
Palácio das Araucárias – Rua Jacy Loureiro de Campos, s/n – 1º andar – Centro Cívico – CEP 80.530-140 – Curitiba – Paraná
(41) 3320 6900 I www.amep.pr.gov.br

I. Migrar as operações para outras unidades;

II. Inativar temporariamente a unidade atingida;

III. Estabelecer trabalho remoto, onde for possível;

IV. Acionar seguro patrimonial;

V. Migrar datacenter;

VI. Estabelecer ambiente em nuvem;

VII. Avaliar recuperação física do ambiente.

4.7.2.3. ERRADICAÇÃO

Não é possível erradicar o cenário de desastre, porém o **TIC do STPP/RMC** devera possuir controles para mitigação do risco de indisponibilidade operacional quais sejam:

I. Datacenter redundante;

II. Serviços críticos em nuvem;

III. Backup;

IV. Plano de Desastre e Recuperação;

V. Comitê de Crise;

VI. Seguro patrimonial.

4.7.2.4. RECUPERAÇÃO

Para a recuperação do ambiente é necessário restabelecer os serviços e operação física. Em virtude dos danos ocasionados pelo desastre poderá ocorrer a inativação de um ambiente.

4.8. SUCESSÃO PLANEJADA (PROPRIEDADE INTELECUTAL)

4.8.1. DEFINIÇÃO

Com o objetivo de assegurar a continuidade dos serviços e a integridade das operações do **STPP/RMC** os **Agentes de TIC do STPP/RMC** deverão implementar processos de sucessão planejada que garantam a preservação e a transferência adequada das informações críticas. Esses processos devem contemplar a manutenção de documentação completa e atualizada sobre atividades essenciais, procedimentos operacionais,

AGÊNCIA DE ASSUNTOS METROPOLITANOS DO PARANÁ – AMEP
Palácio das Araucárias – Rua Jacy Loureiro de Campos, s/n – 1º andar – Centro Cívico – CEP 80.530-140 – Curitiba – Paraná
(41) 3320 6900 I www.amep.pr.gov.br

configurações de sistemas, estrutura e documentação de bancos de dados, bem como backups e registros de alterações, assegurando que tais informações estejam disponíveis para auditoria e entrega ao **PODER CONCEDENTE** sempre que solicitado, visando garantir a continuidade do negócio dentro dos padrões estabelecidos.

Na hipótese de substituição de fornecedor ou término contratual, todas as informações necessárias à continuidade dos serviços deverão ser entregues de forma íntegra e completa, incluindo base de dados atualizada, documentação técnica e funcional e histórico de alterações e customizações. Para garantir a conformidade e a integridade das informações, deverá ser realizada auditoria nos dados recebidos ao final do contrato, acompanhando a transição das bases entre fornecedores, de modo a assegurar que não haja perda ou comprometimento das informações.

O fornecedor de software deverá realizar o depósito do código-fonte junto ao **PODER CONCEDENTE**, exclusivamente como garantia de continuidade do serviço, medida preventiva, alinhada às boas práticas de governança e continuidade (ISO 22301, NIST CSF).

Esse código-fonte será acionado apenas em hipóteses excepcionais, como falência do fornecedor, descontinuidade do negócio ou impossibilidade comprovada de manutenção do serviço, garantindo que outro fornecedor possa assumir a operação sem prejuízo à funcionalidade do sistema.

Além disso, todas as alterações, evoluções e customizações em softwares realizadas a pedido do **PODER CONCEDENTE** ou das **CONCESSIONÁRIAS** serão de propriedade exclusiva do **PODER CONCEDENTE**, devendo ser entregues integralmente, acompanhadas da respectiva documentação técnica e funcional, assegurando que tais desenvolvimentos permaneçam sob controle da Administração Pública.

Na hipótese de descumprimento o **PODER CONCEDENTE** deverá adotar as medidas necessárias para garantir a continuidade do serviço e a proteção do interesse público.

4.8.2. PROCEDIMENTO

4.8.2.1. IDENTIFICAÇÃO

AGÊNCIA DE ASSUNTOS METROPOLITANOS DO PARANÁ – AMEP
Palácio das Araucárias – Rua Jacy Loureiro de Campos, s/n – 1º andar – Centro Cívico – CEP 80.530-140 – Curitiba – Paraná
(41) 3320 6900 I www.amep.pr.gov.br

Devem ser identificados os processos críticos e fornecedores que detenham conhecimento exclusivo, realizando-se mapeamento dos procedimentos integrantes do **TIC do STPP/RMC**.

4.8.2.2. CONTENÇÃO

Após a identificação é necessário realizar as seguintes ações:

I. Realizar o mapeamento do processo ou tarefa crítica;
II. Confeccionar procedimentos e instruções de trabalho;
III. Mapear dados críticos para o sistema;
IV. Realizar o backup;
V. Manter a documentação do processo atualizada;
VI. Manter disponível para todos os envolvidos.

4.8.2.3. ERRADICAÇÃO

Para erradicação do cenário é necessário manter os controles de contenção atualizados e mapear regularmente serviços, processos e fornecedores críticos para a continuidade de negócio.

4.8.2.4. RECUPERAÇÃO

O ambiente que possua planejamento de sucessão será considerado recuperado.

4.9. TERCEIRIZAÇÃO

4.9.1. DEFINIÇÃO

Um fornecedor é uma empresa que fornece produtos ou serviços a outras empresas. Eles são responsáveis por fornecer materiais, mercadorias, equipamentos ou serviços essenciais – o que os torna fundamentais na cadeia de suprimentos de uma organização. No caso do SBE (Sistema de Bilhetagem Eletrônica), por exemplo, com relação à TI temos como principais fornecedores:

I. Datacenter (colocation);
II. Gestor de Tecnologia da Informação;

AGÊNCIA DE ASSUNTOS METROPOLITANOS DO PARANÁ – AMEP
Palácio das Araucárias – Rua Jacy Loureiro de Campos, s/n – 1º andar – Centro Cívico – CEP 80.530-140 – Curitiba – Paraná
(41) 3320 6900 I www.amep.pr.gov.br

III. Fornecedores de nuvem;

IV. Softwares;

V. Equipamentos e ferramentas; e

VI. Demais serviços críticos.

4.9.2. PROCEDIMENTO

4.9.2.1. IDENTIFICAÇÃO

Implementar processo de homologação de fornecedores, definindo requisitos mínimos para operar o **TIC do STPP/RMC** e monitoramento dos serviços prestados. Com esse processo é possível identificar situações potenciais que possam prejudicar a organização ou então causar alguma indisponibilidade.

4.9.2.2. CONTENÇÃO

Através do Processo de Homologação de Fornecedores e do monitoramento das entregas, SLA de atendimento, indisponibilidades e não conformidades são identificadas situações de risco onde podem ser necessários planos de ação.

4.9.2.3. ERRADICAÇÃO

Uma vez implementado o processo de homologação dos fornecedores, com a definição dos requisitos mínimos de monitoramento dos serviços prestados, o risco estará erradicado.

4.9.2.4. RECUPERAÇÃO

A recuperação pode ser realizada com o retorno dos serviços providos pelos fornecedores como também pela substituição de fornecedores, ferramentas e sistemas.

5. TESTE DO PLANO DE DESASTRE

Testes do plano de contenção dos cenários de descontinuidade serão realizados anualmente. Os testes serão registrados nos Plano de Cutover e serão registrados planos de ação para melhoria.

AGÊNCIA DE ASSUNTOS METROPOLITANOS DO PARANÁ – AMEP
Palácio das Araucárias – Rua Jacy Loureiro de Campos, s/n – 1º andar – Centro Cívico – CEP 80.530-140 – Curitiba – Paraná
(41) 3320 6900 I www.amep.pr.gov.br

6. GESTÃO DA MUDANÇA

Sempre que ocorrer uma mudança que tenha impacto sobre a continuidade dos negócios ou continuidade dos serviços do **TIC do STPP/RMC** é necessária a gestão dessa mudança, utilizando o Procedimento Gestão da Mudança para avaliação dos riscos e plano de ação.

AGÊNCIA DE ASSUNTOS METROPOLITANOS DO PARANÁ – AMEP
Palácio das Araucárias – Rua Jacy Loureiro de Campos, s/n – 1º andar – Centro Cívico – CEP 80.530-140 – Curitiba – Paraná
(41) 3320 6900 I www.amep.pr.gov.br

PROCEDIMENTO DE GESTÃO DE ATIVOS, AMEAÇAS E VULNERABILIDADES

1. OBJETIVO

Definir sistemática para gestão de ativos (hardware, software, informação, BYOD, trânsito de informação).

2. RESPONSABILIDADES

2.1. Dos Agentes de TIC do STPP/RMC

I. Assegurar que todos os ativos utilizados no **TIC do STPP/RMC** estejam inventariados sistemicamente;

II. Garantir monitoramento de todos os ativos envolvidos na operação do **TIC do STPP/RMC**;

III. Assegurar o acompanhamento dos alertas de consumo e disponibilidade dos ativos do **TIC do STPP/RMC**;

IV. Assegurar a utilização de ferramentas de proteção de perímetro lógico dos ativos;

V. Garantir o controle de ativos e softwares;

VI. Garantir o tratamento de artefatos maliciosos e vulnerabilidades identificadas.

3. PROCEDIMENTO

3.1. Gestão de Ativos

I. Os **Agentes de TIC do STPP/RMC** devem garantir a gestão e controle dos ativos relacionados a operação, implementando agentes de monitoramento nos computadores ligados ao ambiente operacional que possui acesso aos dados e que as informações serão enviadas para um servidor onde poderão ser acessadas via interface web para auditoria;

II. Devem assegurar que o patrimônio de ativos esteja identificado e inventariado sistemicamente por softwares ou ferramentas de inventários;

III. Garantir a segurança dos ativos físicos operacionais, seja ele por DLP, classificação da informação, BitLocker, duplo fator de autenticação (MFA) entre

AGÊNCIA DE ASSUNTOS METROPOLITANOS DO PARANÁ – AMEP
Palácio das Araucárias – Rua Jacy Loureiro de Campos, s/n – 1º andar – Centro Cívico – CEP 80.530-140 – Curitiba – Paraná
(41) 3320 6900 I www.amep.pr.gov.br

outros;

IV. Devem ainda garantir um inventário de licenças do ambiente com controle de vencimento e provisionamento de novas licenças para novos colaboradores;

V. Garantir que todo usuário que realiza uso dos ativos tenha assinado termo de responsabilidade dos ativos recebidos e sigilo das informações acessadas.

3.2. Servidores

I. Os **Agentes de TIC do STPP/RMC** devem garantir monitoramento nos servidores de operação. As informações serão enviadas para um servidor onde as informações coletadas poderão ser acessadas via interface web para auditoria;

II. Devem garantir que os servidores serão monitorados para acompanhamento e alertas sobre consumo de hardware (CPU, Memória, espaço em disco) e disponibilidade da operação;

III. Garantir a segurança dos servidores operacionais, seja ele por criptografia, duplo fator de autenticação (MFA) entre outros.

3.3. Equipamentos de comutação e ferramentas de perímetros (Firewall, WAF, IPS, Link de internet entre outros)

I. Os **Agentes de TIC do STPP/RMC** devem assegurar a instalação de agentes de monitoramento nos equipamentos de comutação e ferramentas de perímetros. As informações serão enviadas para um servidor onde deverão ser coletadas e poderão ser acessadas via interface web para auditoria;

II. Devem assegurar que os equipamentos serão monitorados para acompanhamento de alertas sobre consumo de hardware (CPU, Memória, espaço em disco) e disponibilidade de operação;

III. Garantir que estes equipamentos estejam configurados segundo as boas práticas de segurança da ferramenta;

IV. Garantir que os ativos e as ferramentas críticas à operação estejam elencadas no Plano de DRP e que possuam redundância para atender a operação em caso de indisponibilidade.

3.4. Gestão de Ameaças e Vulnerabilidades

AGÊNCIA DE ASSUNTOS METROPOLITANOS DO PARANÁ – AMEP
Palácio das Araucárias – Rua Jacy Loureiro de Campos, s/n – 1º andar – Centro Cívico – CEP 80.530-140 – Curitiba – Paraná
(41) 3320 6900 I www.amep.pr.gov.br

Os **Agentes de TIC do STPP/RMC** devem realizar a gestão das vulnerabilidades e ameaças, através de ferramenta especializada em análise dos dados de monitoramento de fontes de segurança de vulnerabilidade, correções, remediações sem patch e ameaças emergentes que correspondem ao software dentro do sistema.

Processo dividido em duas etapas:

Descoberta: é a etapa onde verifica-se, dentro da saúde de gestão de ativos, aquilo que representa o escopo de aplicação de patches pendentes. Devem ser levados em consideração ambientes Microsoft, Linux, ativos de redes e softwares de terceiros;

Identificação: varredura automatizada com auxílio de ferramenta específica.

3.4.1. Correção de Vulnerabilidades:

I. Vulnerabilidades que possuem correção: os **Agentes de TIC do STPP/RMC** devem garantir que serão seguidos os prazos de aplicação de acordo com o nível de criticidade apontado pela ferramenta automatizada ou pelos órgãos de pesquisa, através do processo de atualização de Patches conforme abaixo:

- Nível 5 – em até 15 dias;
- Nível 4 – em até 15 dias;
- Nível 3 – em até 20 dias;
- Nível 2 – em até 20 dias
- Nível 1 – em até 30 dias;

II. Para vulnerabilidades que não existem correções: deverá também ser formalizadas e realizadas avaliações de medidas de controles compensatórios, através de abertura de GMUD.

3.5. Gestão de Patches

I. Os **Agentes de TIC do STPP/RMC** devem garantir a aplicação de patches e realizar a atualização dos sistemas Operacionais Windows e Linux através da utilização de ferramenta de atualização e aplicação de patches de forma automática para todos os equipamentos ingressados na operação;

II. Devem garantir que para os casos de equipamentos de rede como Firewall,

AGÊNCIA DE ASSUNTOS METROPOLITANOS DO PARANÁ – AMEP
Palácio das Araucárias – Rua Jacy Loureiro de Campos, s/n – 1º andar – Centro Cívico – CEP 80.530-140 – Curitiba – Paraná
(41) 3320 6900 I www.amep.pr.gov.br

Roteador, Switch e entre outros, a aplicação de patches deve ocorrer assim que for identificado uma vulnerabilidade;

III. Assegurar que as aplicações de atualizações de sistemas para versões recentes ocorram conforme determinado pelo fabricante.

3.6. Matriz de **responsabilidades** dos ativos

Os **Agentes de TIC do STPP/RMC** devem internamente garantir que todos os envolvidos na gestão de ativos conheçam as suas funções e responsabilidades.

Sigla	Atribuição	Definição	Uso
R	Responsible	Executor(es)	Pode haver vários "R" em uma atividade
A	Accountable	Responsável pelo sucesso da atividade	Deve haver um único "A" em cada atividade
C	Consulted	Pessoa/Equipe consultada antes da execução da atividade	Pode haver vários "C" em uma atividade
I	Informed	Pessoa/Equipe informada antes/durante e/ou depois da atividade	Pode haver vários "I" em uma atividade

Figura 1 – Legenda de entidades matriz RACI

Grupo	Escopo	Agentes	Gestor
Estações	Sistema Operacional	R,C,A	I
Servidores	Sistema Operacional	R,C,A	I
Banco de dados	Sistema Operacional, Backup	R,C,A	I
Aplicação	Aplicações Satélite	I	R,C,A
Ativos de Rede	Switches, Roteadores, Aps, IPS, SIEM e Firewall.	R,C,A	I
Ativos de Rede	Sistema de controle de Acesso (Biometria e câmeras)	R,C,A	I
Ativos de Rede	Demais ativos de rede (Nobreaks, Gerador, entre outros)	R,C,A	I
Demais ativos	Não contemplados anteriormente	R,C,I	R,C,I

AGÊNCIA DE ASSUNTOS METROPOLITANOS DO PARANÁ – AMEP
Palácio das Araucárias – Rua Jacy Loureiro de Campos, s/n – 1º andar – Centro Cívico – CEP 80.530-140 – Curitiba – Paraná
(41) 3320 6900 I www.amep.pr.gov.br

PROCEDIMENTO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

1. OBJETIVO

Sistemática para Gestão de ameaças, vulnerabilidades e tratamento de incidentes de segurança da informação.

2. GENERALIDADES

I. **Incidente:** qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

II. **Artefatos Maliciosos:** Também conhecidos como malwares (malicious software), são programas destinados a executar em um sistema de forma ilícita com o intuito de causar algum dano. Tipos de artefatos maliciosos: Vírus, Worms, Trojan horses, Spywares, Bots, Backdoors;

III. **Vulnerabilidade:** qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores.

3. RESPONSABILIDADES

3.1. DO PODER CONCEDENTE

I. Assegurar a execução do tratamento de incidentes, artefatos maliciosos e vulnerabilidades identificadas na operação do **TIC do STPP/RMC**;

II. Realizar auditoria de conformidade do **TIC do STPP/RMC**.

3.2. DOS AGENTES DE TIC DO STPP/RMC

IV. Assegurar que serão executadas as atividades de tratamento e resposta a incidentes no ambiente operacional;

V. Assegurar a emissão de alertas e advertências relacionadas a incidentes de SI no ambiente operacional;

VI. Garantir a divulgação de forma proativa, de alertas sobre vulnerabilidades e problemas de incidentes de segurança em redes e sistemas no ambiente operacional;

AGÊNCIA DE ASSUNTOS METROPOLITANOS DO PARANÁ – AMEP
Palácio das Araucárias – Rua Jacy Loureiro de Campos, s/n – 1º andar – Centro Cívico – CEP 80.530-140 – Curitiba – Paraná
(41) 3320 6900 I www.amep.pr.gov.br

VII. Garantir a análise detalhada da infraestrutura de segurança em redes e sistemas no ambiente operacional com base nos requisitos do **TIC do STPP/RMC** e nas melhores práticas de SI;

VIII. Assegurar a execução das tarefas que viabilizem ou facilitem a detecção de intrusão;

IX. Garantir a disseminação das informações relacionadas à segurança que sejam ostensivas, facilitem a pesquisa e utilização por todos os membros E;

X. Garantir medidas que visem minimizar os prejuízos causados por falhas e incidentes de SI, e monitoramento de tais incidentes.

4. PROCEDIMENTO

4.1. DISPOSIÇÕES

O Plano de Resposta a Incidentes deve ser visto como um conjunto de procedimentos para avaliação de um incidente de segurança, que inclui preparação, detecção, resposta, contenção, recuperação, comunicação, atividades pós-incidente necessárias, incluindo treinamentos e testes, a ser elaborado em conformidade com a ABNT NBR ISO/IEC 27.035.

4.2. DETALHAMENTO

Estão abrangidos neste procedimento o tratamento de todos os eventos que violem o ambiente de Segurança como, por exemplo:

I. Divulgação não autorizada de dado ou informação sigilosa contida em sistema, arquivo ou base de dados;

II. Invasão de dispositivo informático;

III. Interrupção de serviço telemático ou de informação de utilidade pública;

IV. Inserção ou facilitação de inserção de dados falsos, alteração ou exclusão de dados corretos nos sistemas informatizados ou bancos de dados;

V. Modificação ou alteração por usuário de sistema de informação ou programa de informática sem autorização;

AGÊNCIA DE ASSUNTOS METROPOLITANOS DO PARANÁ – AMEP
Palácio das Araucárias – Rua Jacy Loureiro de Campos, s/n – 1º andar – Centro Cívico – CEP 80.530-140 – Curitiba – Paraná
(41) 3320 6900 I www.amep.pr.gov.br

VI. Distribuição, armazenamento ou conduta vinculada à pornografia infantil;

VII. Interceptação telemática clandestina.

4.3. IDENTIFICAÇÃO DAS FALHAS E INCIDENTES

Os **Agentes de TIC do STPP/RMC** deverão, para minimizar os prejuízos causados por falhas e incidentes de Segurança da Informação, e garantir que tais incidentes sejam monitorados, seguir as seguintes regras:

I. Estabelecer canais de comunicação para incidentes de segurança da informação que sejam de fácil acesso aos seus colaboradores internos e divulgá-los apropriadamente;

II. Atuar proativamente na identificação de potenciais falhas de segurança de informação através dos sistemas de detecção;

III. Assegurar que as pessoas que comunicarem incidentes de SI (Segurança da Informação) sejam informadas dos resultados depois que o incidente tenha sido tratado e encerrado (solucionado ou não);

IV. Utilizar casos de incidentes de segurança da informação e comunicações como exemplo no treinamento de conscientização dos usuários sobre o que poderia acontecer e como reagir a tais incidentes e principalmente, como evitá-los no futuro, desde que respeitando as questões referentes ao nível de sigilo e confidencialidade da informação;

V. Tomar medidas para prevenir a recorrência dos incidentes de SI;

VI. Coletar trilhas de auditoria e evidências similares para embasamento de eventuais processos administrativos, criminais ou judiciais;

VII. Documentar detalhadamente todas as ações de emergência adotadas no tratamento de incidentes de SI.

4.3.1. Serviços prestados pela gestão de Incidentes

SERVIÇO	DESCRIÇÃO
Tratamento de artefatos maliciosos	Este serviço prevê o recebimento de informações ou cópia do artefato malicioso que foi utilizado no ataque, ou em qualquer outra atividade desautorizada ou maliciosa. Uma vez recebido o artefato, o mesmo deve ser analisado, ou seja, deve-

AGÊNCIA DE ASSUNTOS METROPOLITANOS DO PARANÁ – AMEP
Palácio das Araucárias – Rua Jacy Loureiro de Campos, s/n – 1º andar – Centro Cívico – CEP 80.530-140 – Curitiba – Paraná
(41) 3320 6900 I www.amep.pr.gov.br

	se buscar a natureza do artefato, seu mecanismo, versão e objetivo, para que seja desenvolvida, ou pelo menos sugerida, uma estratégia de detecção, remoção e defesa contra estes artefatos. Caso não seja possível determinar a causa ou atacante é necessário realizar investigação forense pós incidentes.
Tratamento de vulnerabilidades	Este serviço prevê o recebimento de informações sobre vulnerabilidades, quer sejam em hardware ou software, objetivando analisar sua natureza, mecanismo e suas consequências, além de desenvolver estratégias para detecção e correção dessas vulnerabilidades.
Emissão de alertas e advertências	Este serviço consiste em divulgar alertas ou advertências imediatas em reação a um incidente de segurança ocorrido em redes de computadores, com o objetivo de advertir a comunidade ou dar orientações sobre como a comunidade deve agir diante do problema.
Anúncios	Este serviço consiste em divulgar, de forma proativa, alertas sobre vulnerabilidades e problemas de incidentes de segurança em redes de computadores em geral, cujos impactos sejam de médio e longo prazo, possibilitando que a comunidade se prepare contra novas ameaças.
Prospecção ou monitoramento de novas	Este serviço prospecta e/ou monitora o uso de novas técnicas das atividades de intrusão e tendências relacionadas, as quais ajudarão a identificar futuras ameaças. Inclui a participação em listas de discussão sobre incidentes de segurança em redes de computadores e o acompanhamento de notícias na mídia em geral sobre o tema.
Avaliação de segurança	Este serviço consiste em efetuar uma análise detalhada da infraestrutura de segurança em redes de computadores da organização com base em requisitos da própria organização ou em melhores práticas de mercado. O serviço pode incluir: revisão da infraestrutura, revisão de processos, varredura da rede e testes de penetração.
Detecção de intrusão	Este serviço prevê a análise do histórico de dispositivos que detectam as tentativas de intrusões em redes de computadores, com vistas a identificar e iniciar os procedimentos de resposta a incidente de segurança em redes de computadores, com base em eventos com características pré-definidas, que possam levar a uma possível intrusão e, ainda, possibilitar o envio de alerta.
Disseminação de informações relacionadas à segurança	Este serviço fornece de maneira fácil e abrangente a possibilidade de encontrar informações úteis no auxílio do tratamento de incidentes de segurança em redes computacionais.

4.3.2. Tratamento e Resposta a Incidente

Com a finalidade de executar as atividades de tratamento e de resposta a incidentes em redes computacionais, os **Agentes de TIC do STPP/RMC** devem:

AGÊNCIA DE ASSUNTOS METROPOLITANOS DO PARANÁ – AMEP
Palácio das Araucárias – Rua Jacy Loureiro de Campos, s/n – 1º andar – Centro Cívico – CEP 80.530-140 – Curitiba – Paraná
(41) 3320 6900 I www.amep.pr.gov.br

I. Registrar todos os incidentes notificados ou detectados no sistema de detecção, a fim de manter um registro histórico de todas as atividades;

II. Investigar as causas dos incidentes de segurança da informação, comunicar e tomar as ações corretivas necessárias;

III. Acionar as autoridades policiais competentes para a adoção dos procedimentos legais julgados necessários;

IV. Observar os procedimentos para preservação das evidências, seguindo a cadeia de custódia:

a) Identificar o incidente, as pessoas envolvidas, abrangência no sistema e o impacto;

b) Conter e isolar o incidente para que ele não se espalhe por todo o **TIC do STPP/RMC**;

c) Eliminar o problema, aplicando as correções levantadas e monitorando para se ter o resultado esperado;

d) Recuperação, como será restabelecido o ambiente afetado e quais sistemas precisam ser reestabelecidos com prioridade;

e) Realizar o histórico das ocorrências do incidente de maneira formal, assim como documentar todos os processos de resposta que erradicaram o incidente mantendo e preservando evidências das ações e da correção, o que vai criar um material como lição apreendida e para o **TIC do STPP/RMC** estar preparado para ataques que possam ocorrer no futuro atualizando o plano de incidentes;

f) Se durante a investigação os dados obtidos na tratativa não possibilitem a identificação do atacante e a origem deste, deve ser avaliada a possibilidade de encaminhar para Investigação Forense por profissionais especializados;

V. Executar uma análise crítica sobre os registros de falhas para assegurar que elas tenham sido satisfatoriamente resolvidas;

VI. Executar uma análise crítica sobre as medidas corretivas adotadas para assegurar que não tenham ocorrido comprometimentos (criação de vulnerabilidades) na execução de medidas para solucionar um incidente de Segurança da Informação e que as ações tenham sido devidamente autorizadas;

AGÊNCIA DE ASSUNTOS METROPOLITANOS DO PARANÁ – AMEP
Palácio das Araucárias – Rua Jacy Loureiro de Campos, s/n – 1º andar – Centro Cívico – CEP 80.530-140 – Curitiba – Paraná
(41) 3320 6900 I www.amep.pr.gov.br

VII. Implementar mecanismos para permitir a quantificação e monitoramento dos tipos, volumes, custos de incidentes e de falhas de funcionamento (ex. ferramenta de monitoramento de alertas IDR);

VIII. Identificar incidentes ou falhas repetidas ou de alto impacto, isto é, incidentes que possam acarretar graves riscos ao negócio ou que atinjam um grande contingente de usuários;

IX. Indicar a necessidade de controles aperfeiçoados ou adicionais para limitar a frequência, os danos e o custo de futuras ocorrências de incidentes;

X. Observar a legislação em vigor e as normativas internas no tratamento de informações classificadas com algum nível de sigilo, de forma a viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação sob posse ou custódia.

4.3.3. SLA de Incidente

4.3.3.1. Os **Agentes de TIC do STPP/RMC** devem garantir a análise dos dados coletados sistemicamente via ferramenta de monitoramento no ambiente e em caso de identificação de um incidente possuir resposta imediata para aplicação do protocolo de Identificação, Contenção, Erradicação, Recuperação e Documentação para Lição aprendida.

Figura: Processo de Tratamento de Incidentes.

4.4. COMUNICAÇÃO DOS INCIDENTES DE SEGURANÇA

AGÊNCIA DE ASSUNTOS METROPOLITANOS DO PARANÁ – AMEP
Palácio das Araucárias – Rua Jacy Loureiro de Campos, s/n – 1º andar – Centro Cívico – CEP 80.530-140 – Curitiba – Paraná
(41) 3320 6900 I www.amep.pr.gov.br

Os **Agentes de TIC do STPP/RMC** devem garantir que a comunicação dos incidentes de segurança, vulnerabilidades percebidas e demais eventos de segurança se dará por meio formal que permita os registros desses comunicados e incidentes.

Na ocorrência de um incidente de segurança com vazamento de dados pessoais a organização deve atuar no incidente para contenção e gerar os procedimentos para comunicar a ANPD e aos titulares dos dados vazados seguindo o plano de comunicação com o usuário do **STPP/RMC**.

4.5. TESTE DE SEGURANÇA

Os **Agentes de TIC do STPP/RMC** devem assegurar a realização de testes periódicos, para verificar o grau de segurança alcançado pelas medidas adotadas para proteção do ambiente, sendo vedado aos usuários dos recursos computacionais tentar provar um ponto fraco de que suspeite, a não ser que seja autorizado pelo agente contratante, o teste de um ponto fraco sem autorização expressa pode ser interpretado como um uso abusivo do sistema.

4.6. REQUISITOS PARA ADEQUAÇÃO DOS ATIVOS DE INFORMAÇÃO

Os **Agentes de TIC do STPP/RMC** devem garantir que o horário dos ativos de informação, estejam ajustados por meio de um mecanismo de sincronização de tempo, de forma a garantir que as configurações de data, hora e fuso horário do relógio interno estejam sincronizados com a “Hora Legal Brasileira (HLB)”, de acordo com o serviço oferecido e assegurado pelo Observatório Nacional (ON).

Os ativos de informação devem ser configurados de forma a registrar todos os eventos relevantes de SI e no mínimo, os seguintes:

I. Autenticação, tanto os bem-sucedidos quanto os mal-sucedidos;

II. Acesso a recursos e dados privilegiados; e

III. Acesso e alteração nos registros de auditoria.

IV. Os registros dos eventos previstos anteriormente devem incluir as seguintes informações:

AGÊNCIA DE ASSUNTOS METROPOLITANOS DO PARANÁ – AMEP
Palácio das Araucárias – Rua Jacy Loureiro de Campos, s/n – 1º andar – Centro Cívico – CEP 80.530-140 – Curitiba – Paraná
(41) 3320 6900 I www.amep.pr.gov.br

V. Identificação inequívoca do usuário que acessou o recurso;

VI. Natureza do evento, como sucesso ou falha de autenticação, tentativa de troca de senha entre outros;

VII. Data, hora e fuso horário;

VIII. Endereço IP (Internet Protocol), identificador do ativo de informação, coordenadas geográficas, se disponíveis e outras informações que possam identificar a possível origem do evento.

Os ativos de informação que não permitam os registros de eventos acima listados devem ser mapeados e documentados quanto ao tipo e formato de registros de auditoria que o sistema permita armazenar. Devem-se acompanhar os sistemas e redes de comunicação de dados, registrando-se os eventos de segurança elencados abaixo, sem prejuízo de outros considerados relevantes:

I. Utilização de usuários, perfis e grupos privilegiados;

II. Inicialização, suspensão e reinicialização de serviços;

III. Acoplamento e desacoplamento de dispositivos de hardware, com atenção às mídias removíveis;

IV. Modificações de política de senhas, como por exemplo, tamanho, expiração, bloqueio automático após exceder determinado número de tentativas de autenticação, histórico entre outros;

V. Acesso ou modificação de arquivos ou sistemas considerados críticos; e

VI. Eventos obtidos de quaisquer mecanismos de segurança existentes.

Os servidores de hospedagem de página eletrônica, bem como todo e qualquer outro ativo de informação que assim o permita, devem ser configurados para armazenar registros históricos de eventos (Logs) em formato que permita a completa identificação dos fluxos de dados.

Os registros devem ser preservados conforme Procedimento de Registro de Operações.

4.7. CONTATO COM AUTORIDADES E GRUPOS ESPECIAIS

AGÊNCIA DE ASSUNTOS METROPOLITANOS DO PARANÁ – AMEP
Palácio das Araucárias – Rua Jacy Loureiro de Campos, s/n – 1º andar – Centro Cívico – CEP 80.530-140 – Curitiba – Paraná
(41) 3320 6900 I www.amep.pr.gov.br

Os **Agentes de TIC do STPP/RMC** devem manter contatos apropriados com autoridades relevantes, caso ocorram incidentes de segurança da informação, como grupos de resposta a incidentes.

Devem buscar fazer parte de Comitês de Segurança da Informação para manter-se sempre atualizados das vulnerabilidades e indisponibilidade do setor, como grupo de resposta a incidente CSIRT, NIC, ANPD entre outros.

AGÊNCIA DE ASSUNTOS METROPOLITANOS DO PARANÁ – AMEP
Palácio das Araucárias – Rua Jacy Loureiro de Campos, s/n – 1º andar – Centro Cívico – CEP 80.530-140 – Curitiba – Paraná
(41) 3320 6900 I www.amep.pr.gov.br

PROCEDIMENTO DE CONTROLE DE ACESSO FÍSICO

1. OBJETIVO

Definir sistemática para controle de acesso.

2. GENERALIDADE

CFTV: Circuito fechado de televisão ou circuito interno de televisão é um sistema de televisão que distribui sinais provenientes de câmeras localizadas em locais específicos, para um ou mais pontos de visualização;

LOG de Dados: é uma expressão utilizada para descrever o processo de registro de eventos relevantes num sistema computacional.

3. RESPONSABILIDADES

3.1. DOS AGENTES DE TIC DO STPP/RMC

I. Garantir que as suas instalações físicas e lógicas possuam estrutura de segurança adequada para salvaguardar os dados por ela transitados ou armazenados;

II. Assegurar que as áreas críticas de operação onde concentram a maior quantidade de dados do **TIC do STPP/RMC** possuam restrição de acesso indevido;

III. Assegurar que todos os acessos ao seu ambiente físico e lógico sejam monitorados de forma proativa.

4. PROCEDIMENTO

4.1. CONTROLE DE ACESSO FÍSICO

I. Os **Agentes de TIC do STPP/RMC** devem garantir controle de acesso físico a suas instalações, seja ele por colaboradores, prestadores de serviços, fornecedores e terceiros, determinando os critérios para cada acesso e seus devidos meios de monitoramento;

II. Devem garantir que o controle de acessos mantenha registros para auditorias independentes do Poder Concedente, forneça relatórios de entradas e saídas contendo horário (oficial de Brasília), identificação e registro de Log da aplicação;

AGÊNCIA DE ASSUNTOS METROPOLITANOS DO PARANÁ – AMEP
Palácio das Araucárias – Rua Jacy Loureiro de Campos, s/n – 1º andar – Centro Cívico – CEP 80.530-140 – Curitiba – Paraná
(41) 3320 6900 I www.amep.pr.gov.br

4.1.1. COLABORADORES

I. Os **Agentes de TIC do STPP/RMC** devem gerenciar os acessos aos setores e as áreas sensíveis (grande volume de dados sensíveis) da organização e estas áreas devem ser segregadas com acesso físico restrito, seja por acesso via crachá, biometria ou fechadura digital;

II. Devem garantir que ao admitir um colaborador este seja incluso no controle de acessos e tenha seus devidos permissionamentos liberados e na ocorrência de afastamento, férias ou desligamento o controle de acessos tseja atualizado retirando-se imediatamenteas permissões a o ambiente físico do agente, de tal maneira que fique inacessível ao ex-colaborador.

4.1.2. VISITANTES, PRESTADORES DE SERVIÇOS, FORNECEDORES E TERCEIROS

Os **Agentes de TIC do STPP/RMC** devem garantir que os acessos de visitantes, prestadores de serviços, fornecedores e terceiros ao ambiente do **TIC do STPP/RMC** sejam registrados e acompanhados durante todo o período em que estes permanecerem no ambiente físico.

Devem ser identificados, registrados no controle de acessos e liberados somente sob supervisão e acompanhamento da área receptora na área de entrada. Não deve ser permitida a entrada desassistida as áreas de forma deliberada.

4.1.3. HORÁRIO

Os **Agentes de TIC do STPP/RMC** devem estabelecer controle do horário de trabalho e atendimento em suas operações. Acessos realizados fora do horário de expediente, devem ser formalmente liberados e registrados via sistema de acordo com os acessos de cada colaborador.

4.2. CLASSIFICAÇÃO DAS ÁREAS

Os **Agentes de TIC do STPP/RMC** devem mapear e classificar suas áreas com alto, média e baixo risco de vazamento de informações e as restrições de acesso.

AGÊNCIA DE ASSUNTOS METROPOLITANOS DO PARANÁ – AMEP
Palácio das Araucárias – Rua Jacy Loureiro de Campos, s/n – 1º andar – Centro Cívico – CEP 80.530-140 – Curitiba – Paraná
(41) 3320 6900 I www.amep.pr.gov.br

4.3. REGISTROS DE ACESSOS

Os **Agentes de TIC do STPP/RMC** devem manter registro do controle de acesso as instalações, bem como recomenda-se registro via sistemas de segurança como alarmes e monitoramento de CFTV, com informações de como são acessados, quem recebe o acionamento em caso de alerta e local de armazenamento dos relatórios gerados por períodos.

4.4. DATA CENTER E SERVIDORES

Os **Agentes de TIC do STPP/RMC** devem garantir que o acesso ao Data Center e Servidores, seja ainda mais restrito com controle de acesso biométrico e possua implementado os controles de segurança adequados para manter a operação. Os registros dos acessos, inclusive de visitantes, devem gravados para gerar relatórios e devem ser salvos para apresentá-los em auditoria.

AGÊNCIA DE ASSUNTOS METROPOLITANOS DO PARANÁ – AMEP
Palácio das Araucárias – Rua Jacy Loureiro de Campos, s/n – 1º andar – Centro Cívico – CEP 80.530-140 – Curitiba – Paraná
(41) 3320 6900 I www.amep.pr.gov.br

PROCEDIMENTO DE GESTÃO DE MUDANÇA

1. OBJETIVO

Definir o Processo de Gerenciamento de Mudanças a ser utilizado na operação do **TIC do STPP/RMC**.

2. DEFINIÇÕES

RFC: Request for Change ou em tradução livre "requisição de mudança";
Rollback: refere-se à atividade de desfazer todas as mudanças realizadas no "ambiente" de forma que volte a ter as mesmas características de antes das mudanças.

3. RESPONSABILIDADES

3.1. DOS AGENTES DE TIC DO STPP/RMC

I. Analisar, aprovar, rejeitar, priorizar e autorizar as mudanças encaminhadas de forma conjunta;

II. Garantir que as mudanças realizadas no ambiente do **TIC do STPP/RMC** serão analisadas para minimizar os impactos da operação;

III. Garantir recursos para a execução das atividades do processo de mudança;

IV. Assegurar que as mudanças seguirão o fluxo análise, validação, aprovação ou rejeição;

V. Priorizar as mudanças sob a ótica de segurança da informação;

VI. Assegurar que somente mudanças aprovadas entrem no processo.

3.2. GERENTE DE MUDANÇA OU LÍDER DA ÁREA DA MUDANÇA.

I. Avaliar capacidade de execução e rollback;

II. Avaliar público-alvo para comunicação adequado para cada tipo de mudança (abrangência);

III. Provisionar necessidades para suportar o ambiente durante mudança e efeitos de insucesso;

IV. Avaliar juntamente com dono do processo o impacto e probabilidade dos riscos que serão apontados na RFC;

AGÊNCIA DE ASSUNTOS METROPOLITANOS DO PARANÁ – AMEP
Palácio das Araucárias – Rua Jacy Loureiro de Campos, s/n – 1º andar – Centro Cívico – CEP 80.530-140 – Curitiba – Paraná
(41) 3320 6900 I www.amep.pr.gov.br

V. Comunicar adequadamente a respeito de janelas e indisponibilidades;

VI. Comunicar adequadamente a respeito do andamento de implantação de mudanças e rollbacks;

VII. Realizar gestão de indicadores de mudanças, se aplicável;

VIII. Sanar restrições para a execução do processo.

3.3. TÉCNICO EXECUTOR

I. Executar as atividades programadas;

II. Comunicar gerente da mudança se houver a respeito de sucesso ou insucesso;

III. Fornecer feedback técnico a respeito das mudanças realizadas e não realizadas afim de produzir aprendizado.

3.4. DONOS DE PROCESSOS OU DE SISTEMAS

I. Abrir a requisição de mudança;

II. Realizar correção se necessário da requisição de mudança;

III. Defender a real necessidade da mudança perante o **Agente de TIC do STPP/RMC**;

IV. Encerrar a requisição da mudança;

V. Estabelecer critérios de teste e aceitação dos ambientes após a mudança;

VI. Participar dos testes e aceitação após a mudança realizada;

VII. Validar o ambiente para liberar seu uso;

VIII. Decidir pelo rollback (podendo escalar para o gestor da mudança);

IX. Garantir a correta execução do processo;

X. Garantir a integração com os demais processos desenvolvidos;

XI. Garantir a documentação dos processos e sistemas após mudança;

XII. Garantir a comunicação a respeito dos novos processos após a mudança.

4. PROCEDIMENTO

Os **Agentes de TIC do STPP/RMC** devem garantir que toda mudança efetuada na organização precisa ser gerida para que as novas ações:

I. Não causem interrupções das atividades exercidas pelo **TIC do STPP/RMC**;

AGÊNCIA DE ASSUNTOS METROPOLITANOS DO PARANÁ – AMEP
Palácio das Araucárias – Rua Jacy Loureiro de Campos, s/n – 1º andar – Centro Cívico – CEP 80.530-140 – Curitiba – Paraná
(41) 3320 6900 I www.amep.pr.gov.br

II. Não causem degradação indesejada ou não planejada de capacidade ou desempenho dos serviços e sistemas;

III. Mantenham o bom funcionamento dos sistemas e serviços existentes, entregando resultados esperados e anteriormente planejados;

IV. Tenham como objetivo priorizar e adequar as necessidades de mudança, reduzir os riscos de possíveis rupturas no nível de serviço prestado, otimizar os custos e reduzir o retrabalho através do planejamento, acompanhamento e rastreabilidade do processo e das requisições feitas.

4.1. DIRETRIZES DE MUDANÇA

I. Os **Agentes de TIC do STPP/RMC** devem assegurar que para toda implantação, modificação, remoção de ferramenta / sistema ou processo que impactem em riscos de processo ou segurança da informação de dados deve ser aberta uma RFC;

II. Devem assegurar que todos os riscos foram identificados, avaliados e mitigados sempre que possível durante o planejamento da implantação.

III. Dever garantir que toda RFC está associada com pelo menos um registro de incidente, problema, melhoria ou requisição de serviço.

4.2. GERENCIAMENTO DA MUDANÇA

Para implantar a gestão de mudanças no sistema do **STPP/RMC** é fundamental definir os critérios e as pessoas chave para realização:

I. Responsável pela execução da mudança?

II. Quais os aprovadores Gestor da Mudança ou do Comitê de Segurança da Informação (se houver)?

III. Definição de dias e horários para execução das janelas de mudança?

4.3. ABERTURA DE RFC

Os **Agentes de TIC do STPP/RMC** devem garantir que será aberto uma requisição formal, sugerindo-se formulário com procedimento operacional de mudanças preenchido com os itens a seguir:

I. Escopo da mudança;

II. Objetivo da mudança;

III. Gerenciamento de recursos (tempo, pessoas, ferramental, entre outros);

IV. Avaliação de conformidade para rastreabilidade (log centralizado);

V. Quais setores afetados;

VI. Quais os responsáveis pela mudança;

VII. Plano de comunicação;

VIII. Planejamento das atividades de mudanças;

IX. Execução simulada;

X. Plano de Rollback;

XI. Garantir registro das atividades durante mudanças;

XII. Identificar o evento (incidente, requisição de serviço, problema, melhoria, entre outros) gerador da mudança e vinculá-lo à RFC a ser registrada.

4.4. TIPOS DE MUDANÇAS

Os agentes devem garantir que as RFCs tenham um escopo claramente definido e documentado. Para tanto, o tipo de mudança deve ser registrado de forma correta no momento da abertura da RFC, deve-se considerar pontos como:

I. Complexidade;

II. Pessoas;

III. Exposição;

IV. Falhas;

V. Melhorias;

VI. Usuários envolvidos e quantidade;

4.4.1. Tipo Emergencial

I. Necessidade de restabelecimento rápido, a fim de minimizar ou evitar os impactos para o negócio, tem sua natureza advinda de um incidente crítico;

II. Todas as mudanças emergenciais ocorridas devem ser documentadas, mesmo que seja após sua execução e implantação, a fim de manter-se o rastreio de todas as operações e modificações realizadas.

AGÊNCIA DE ASSUNTOS METROPOLITANOS DO PARANÁ – AMEP
Palácio das Araucárias – Rua Jacy Loureiro de Campos, s/n – 1º andar – Centro Cívico – CEP 80.530-140 – Curitiba – Paraná
(41) 3320 6900 I www.amep.pr.gov.br

4.4.2. Normal

Ocorre na implementação de um processo, serviço ou mão de obra que não possui script de execução e não é classificada como Padrão, precisa ser planejada e autorizada a execução seguindo os procedimentos normais de uma RFC.

4.4.3. Padrão

Mudança em um serviço ou infraestrutura de rotina já pré-autorizada pelo Gestor ou Comitê de Segurança da Informação (se houver) e com um script de procedimento para execução estabelecido.

Os pré-requisitos para uma mudança ser considerada padrão são:

I. A mudança deve ter baixo impacto;

II. A mudança deve ter baixo risco ou risco bem conhecido;

III. Existir um gatilho claramente definido que inicia a mudança;

IV. A mudança deve ter sido fechada com sucesso;

V. A mudança deve ser realizada com frequência e com sucesso.

4.5. PRIORIDADE DAS MUDANÇAS

I. A prioridade das mudanças será definida de acordo com seu impacto e urgência de execução avaliadas pelo Gestor ou Comitê de mudança, se houver;

II. Impacto;

III. Alto: Impacto severo a usuário(s)-chave (alta direção) ou muitos usuários;

IV. Médio/normal: Parcialmente alguns usuários;

V. Baixo: baixo impacto de um recurso, sistema, serviço ou processo;

VI. Mudança de simples execução, que possui atividades padronizadas e conhecidas pelas áreas operacionais.

4.5.1. Urgência

I. Alta: ação imediata é requerida;

II. Média/normal: sem grande urgência, porém a mudança não pode ser adiada para outro instante mais conveniente;

III. Baixa: a mudança precisa ser realizada, porém pode obedecer a agenda de

AGÊNCIA DE ASSUNTOS METROPOLITANOS DO PARANÁ – AMEP
Palácio das Araucárias – Rua Jacy Loureiro de Campos, s/n – 1º andar – Centro Cívico – CEP 80.530-140 – Curitiba – Paraná
(41) 3320 6900 I www.amep.pr.gov.br

mudança.

4.6. PLANO DE COMUNICAÇÃO

I. Os **Agentes de TIC do STPP/RMC** devem informar na RFC quais pessoas e áreas devem ser comunicadas sobre a mudança que ocorrerá, considerando o impacto e indisponibilidade que podem ocorrer;

II. Devem assegurar que toda RFC aprovada irá gerar uma notificação a todos os envolvidos e impactados, informando sobre a mudança e a janela de manutenção implantada.

4.7. JANELA DE APLICAÇÃO DA MUDANÇA GMUD

I. As janelas de mudanças devem ser planejadas para impactar o mínimo possível as operações desenvolvidas;

II. As aplicações e aprovações poderão seguir os ritos da tabela a seguir descrita:

Categoria	Descrição	Aplicação	Aprovador
Emergencial	Quando o ambiente se encontra fora de operação ou amplamente impactado.	Imediatamente após aprovação.	Gestor de TI ou acima.
Urgente	Ambiente parcialmente comprometido. Deve-se aplicar na próxima janela prevista.	No dia da aprovação fora do horário comercial.	Gestor da mudança.
Prevista	Atividades de rotinas que necessitam de planejamento prévio.	Conforme planejamento da RFC.	Gestor da mudança.

4.8. PLANO DE RETORNO (ROLLBACK)

I. Os **Agentes de TIC do STPP/RMC** devem realizar um plano de ação para os casos em que ocorram falhas na implantação, incluindo os meios para restauração das funcionalidades;

II. Devem especificar as atividades de rollback e os responsáveis por executá-las;

III. Devem definir o tempo para realizar o rollback no sistema;

IV. Devem testar o plano de rollback e sua efetividade;

V. Devem assegurar pontos de backup das informações e restore.

AGÊNCIA DE ASSUNTOS METROPOLITANOS DO PARANÁ – AMEP
Palácio das Araucárias – Rua Jacy Loureiro de Campos, s/n – 1º andar – Centro Cívico – CEP 80.530-140 – Curitiba – Paraná
(41) 3320 6900 I www.amep.pr.gov.br

PROCEDIMENTO DE BACKUP

1. OBJETIVO

Definir sistemática de backup dos dados necessários para a realização da operação do **TIC do STPP/RMC**.

2. DEFINIÇÕES

Backup: Termo utilizado para uma atividade que consiste em realizar cópias de segurança de dados digitais de um dispositivo, como fotos, documentos, softwares ou qualquer arquivo digital, com o intuito de recuperá-los em caso de perdas acidentais ou falhas no sistema em que os arquivos estão armazenados.

Auditoria de banco de dados: Realizada para evitar e identificar ações indevidas por parte do usuário através de seus acessos aos dados. Informações sobre os acessos da base de dados são coletadas e analisadas para que se possa descobrir falhas de segurança e a origem do problema.

Restore (Restaurar): Ação de reativar todos os dados que haviam sido salvos no backup. Muitos sistemas, inclusive, contam com a possibilidade de fazer a restauração de diferentes versões previamente armazenadas.

Teste de backup: Verificação de restore (recuperação) é um dos principais focos do teste de backup, que nada mais é do que um processo periódico para verificar a eficácia da criação, do armazenamento e da restauração das cópias de segurança.

3. RESPONSABILIDADES

3.1. DO PODER CONCEDENTE

Garantir que o **TIC do STPP/RMC** passe por auditoria regularmente para manter a saúde dos dados coletados e armazenados.

3.2. DOS AGENTES DE TIC DO STPP/RMC

I. Assegurar que todas as informações estejam salvaguardadas em backup;

II. Garantir cópias anuais do banco de dados em meio imutável para realização de

AGÊNCIA DE ASSUNTOS METROPOLITANOS DO PARANÁ – AMEP
Palácio das Araucárias – Rua Jacy Loureiro de Campos, s/n – 1º andar – Centro Cívico – CEP 80.530-140 – Curitiba – Paraná
(41) 3320 6900 I www.amep.pr.gov.br

auditoria pelo **PODER CONCEDENTE** sem data de expiração;

III. Assegurar que cópias dos backups gerados possuam meios de segurança dos dados em repouso como, por exemplo, criptografia;

IV. Realizar testes de backup (restore), testes periódicos de eficácia e segurança de suas cópias de restauração, observados os seguintes prazos máximos:

a) **Verificação de integridade técnica:** diária e automatizada;

b) **Testes de restauração por amostragem de dados:** mensal;

c) **Testes de segurança e isolamento de redes de armazenamento:** trimestral;

d) **Simulado completo de desastre e restauração sistêmica estrutural (DRP):** semestral, devendo os relatórios de conformidade e resultados ficarem à disposição do **PODER CONCEDENTE** para fins de auditoria.

4. PROCEDIMENTO

4.1. DIRETRIZES GERAIS DE BACKUP

I. Os **Agentes de TIC do STPP/RMC** devem especificar quais os dados serão realizados backups, com ordem de prioridade de dados como, por exemplo, dados de clientes, sistemas críticos, operacionais, base de dados, entre outros e meios de armazenamento físico em fita, disco rígido, cloud, imutável;

II. Garantir backup completo 1 vez ao ano com armazenamento imutável e permanente para auditoria;

III. Garantir backup incremental subsequente ou diferencial dos dados;

IV. Assegurar armazenamento de backup em um local remoto e seguro, a uma distância suficiente para escapar de qualquer dano causado por um desastre no local principal;

V. Assegurar redundância de armazenamento dos dados e Plano de contingência.

4.2. Diretrizes Gerais de Restore

I. Os **Agentes de TIC do STPP/RMC** devem garantir a realização de testes de Restore dos backups das informações utilizadas pelo **TIC do STPP/RMC**

AGÊNCIA DE ASSUNTOS METROPOLITANOS DO PARANÁ – AMEP
Palácio das Araucárias – Rua Jacy Loureiro de Campos, s/n – 1º andar – Centro Cívico – CEP 80.530-140 – Curitiba – Paraná
(41) 3320 6900 I www.amep.pr.gov.br

periodicamente;

II. Devem assegurar o registro desses testes realizados;

III. Garantir a integridade dos dados contidos no backup.

Ainda quanto a Backups Operacionais (servidores e sistemas) deverão ser realizados backups diários (incrementais) com retenção de 14 a 30 dias, enquanto que os backups semanais (cheios) deverão ter retenção mínima de 5 semanas, por sua vez os backups mensais deverão possuir retenção mínima de 12 meses.

Quanto a dados críticos e fiscais como dados de bilhetagem eletrônica, transações financeiras de venda de créditos, dados de auditoria de catracas e logs de validação, que possuem natureza jurídica e fiscal mais sensível, deverá ser observada a retenção de longo prazo, que significa a retenção anualizada por um período mínimo de 5 anos, para fins de prescrição fiscal e guarda de documentos de prestação de contas públicas.

Ainda, sobre logs de segurança e auditoria (SIEM/Logs de Acesso) que são informações essenciais para a análise forense em casos de incidentes cibernéticos ou vazamentos de dados protegidos pela legislação, no que concerne a logs ativos (hot/warm storage) deverá ser armazenado pelo período mínimo de 90 dias, com possibilidade de consulta em sistemas de monitoramento, sendo que os logs arquivados (cold storage/backup) terão prazo mínimo de 18 meses.

AGÊNCIA DE ASSUNTOS METROPOLITANOS DO PARANÁ – AMEP
Palácio das Araucárias – Rua Jacy Loureiro de Campos, s/n – 1º andar – Centro Cívico – CEP 80.530-140 – Curitiba – Paraná
(41) 3320 6900 I www.amep.pr.gov.br

PROCEDIMENTO DE REGISTRO DE OPERAÇÕES

1. OBJETIVO

Definir sistemática para registro de operações de segurança das informações dos sistemas.

2. DEFINIÇÃO

Log - Um arquivo de log é um registro contínuo, que contém a data e a hora do evento, além de uma mensagem criada automaticamente pelos softwares e sistemas de TI. Os logs são registros das ações realizadas nos sistemas

3. RESPONSABILIDADES

3.1. DOS AGENTES DE TIC DO STPP/RMC

I. Cumprir a **Política de Governança de Dados e Segurança** e o procedimento de Registro de Operações;

II. Garantir registro de operação dos sistemas e serviços do **TIC do STPP/RMC**;

III. Garantir disponibilidade e integridade dos registros de operação para auditoria do Poder Concedente;

IV. Garantir a guarda da informação do log pelo período mínimo de 5 (cinco) anos;

V. Assegurar a segurança da informação dos registros de operação armazenados.

4. PROCEDIMENTO

4.1. REGISTRO DE OPERAÇÕES

I. Os **Agentes de TIC do STPP/RMC** devem garantir que o trânsito de Informações seja realizado por um caminho ou meio confiável com controles que ofereçam autenticidade do conteúdo, proteção de submissão, recebimento e não repúdio da origem;

II. Devem determinar mecanismos que permitam registros de acessos aos ambientes, indicando, minimamente e sempre que possível, os recursos acessados, quem efetuou o acesso, data e hora, tentativas de acesso com senhas erradas, tentativas

AGÊNCIA DE ASSUNTOS METROPOLITANOS DO PARANÁ – AMEP
Palácio das Araucárias – Rua Jacy Loureiro de Campos, s/n – 1º andar – Centro Cívico – CEP 80.530-140 – Curitiba – Paraná
(41) 3320 6900 I www.amep.pr.gov.br

de acesso de estações de trabalho não permitidas, tentativas de acesso em horários não permitidos entre outros;

III. Devem relacionar as principais ferramentas operacionais dos sistemas destacando: onde os registros de logs estão armazenados, por quanto tempo e como ter acesso à informação para auditoria.

4.2. LOGS DE SISTEMA

Os **Agentes de TIC do STPP/RMC** devem garantir que logs de eventos a nível de sistema operacional dos servidores, deverão ser monitorados e registrados observando os seguintes elementos:

I. Atividades dos administradores do sistema;
II. Início e desligamento do sistema operacional;
III. Início e encerramento das atividades de log;
IV. Atividades de backup e restore;
V. Eventos de segurança e exceções do sistema;
VI. Modificação de conteúdo, incluindo permissões, tipos de arquivo e diretórios;
VII. Atividades de autenticação – falha ou sucesso em eventos de logon/logoff.

4.3. LOG DE APLICAÇÕES

Os **Agentes de TIC do STPP/RMC** devem garantir o registro e o monitoramento dos logs de aplicações para auxiliar na detecção, investigação e prevenção de incidentes de segurança.

Os registros das aplicações desenvolvidas internamente, bem como as de terceiros, cuja hospedagem esteja sendo realizada na infraestrutura interna, deverão ser monitoradas e registradas, observando os seguintes elementos:

I. Eventos de autenticação – sucesso e falha em logon/logoff;
II. Trilha de auditoria de informações sensíveis – atividades de criação, modificação e exclusão de dados;
III. Falhas na validação de Entradas – violações de protocolos, formato incorreto, parâmetros incorretos;

AGÊNCIA DE ASSUNTOS METROPOLITANOS DO PARANÁ – AMEP
Palácio das Araucárias – Rua Jacy Loureiro de Campos, s/n – 1º andar – Centro Cívico – CEP 80.530-140 – Curitiba – Paraná
(41) 3320 6900 I www.amep.pr.gov.br

IV. Falhas na validação de Saídas – formato inválido, incompatibilidade de registro de banco de dados;

V. Comportamento suspeito – sucessivas tentativas de logon inválidas, múltiplos registros deletados em um curto período;

VI. Falha no gerenciamento da sessão – modificação nos valores de identificação de cookies;

VII. Falha na aplicação ou eventos de falha – erros de execução ou sintaxe, problemas de conectividade, erro no sistema de arquivos, erros de sequenciamento;

VIII. Funcionalidades críticas de sistema – emissão de relatórios, gerenciamento de usuários, mudança de privilégios, acesso de administradores;

IX. Eventos de segurança ou avisos do sistema.

4.4. ELEMENTOS DE LOG

Os **Agentes de TIC do STPP/RMC** devem garantir que os registros de log contenham uma série de elementos básicos para processamento:

I. Hostname: Componente de Serviço ou Recurso;

II. Data;

III. Nome da Aplicação ou ID: nome e versão;

IV. Origem do evento: URL, formulário, página;

V. Usuário iniciando o evento: nome ou ID;

VI. Tipo do evento;

VII. Status do resultado da ação: sucesso ou falha;

VIII. Recurso: identidade ou nome do dado ou componente;

IX. Localização: dados como IP e geolocalização do usuário;

X. Severidade do evento: informação, aviso ou erro.

AGÊNCIA DE ASSUNTOS METROPOLITANOS DO PARANÁ – AMEP
Palácio das Araucárias – Rua Jacy Loureiro de Campos, s/n – 1º andar – Centro Cívico – CEP 80.530-140 – Curitiba – Paraná
(41) 3320 6900 I www.amep.pr.gov.br

PROCEDIMENTO DE CLASSIFICAÇÃO DA INFORMAÇÃO

1. OBJETIVO

Definir sistemática para garantir que as informações do **TIC do STPP/RMC** estejam protegidas adequadamente.

2. RESPONSABILIDADES

Este procedimento aplica-se ao **TIC do STPP/RMC** e todas as organizações que o compõe, a todos os tipos de informações, independentemente do formato (documentos em papel ou formato eletrônico, aplicativos e bancos de dados, conhecimentos de pessoas e outros formatos).

3. GENERALIDADES

Usuários: Estão inclusos no grupo de usuários todas as pessoas que utilizam os sistemas de informação do **TIC do STPP/RMC** (colaboradores, prestadores de serviços, terceiros e fornecedores).

4. RESPONSABILIDADES

4.1. DOS AGENTES DE TIC DO STPP/RMC

I. Garantir que os ativos de informações foram inventariados;

II. Garantir a utilização da classificação e bloqueio de dados em trânsito;

III. Assegurar a utilização de rótulos das Informações.

5. PROCEDIMENTO

5.1. INFORMAÇÃO CLASSIFICADA

Se informações classificadas forem recebidas de fora do **TIC do STPP/RMC**, o destinatário da informação torna-se responsável por sua classificação.

5.2. CLASSIFICAÇÃO DE INFORMAÇÕES

5.2.1. CRITÉRIOS DE CLASSIFICAÇÃO

AGÊNCIA DE ASSUNTOS METROPOLITANOS DO PARANÁ – AMEP
Palácio das Araucárias – Rua Jacy Loureiro de Campos, s/n – 1º andar – Centro Cívico – CEP 80.530-140 – Curitiba – Paraná
(41) 3320 6900 I www.amep.pr.gov.br

Os **Agentes de TIC do STPP/RMC** devem avaliar o nível de confidencialidade com base nos seguintes critérios:

I. Valor da Informação: Impactos analisados durante avaliação de riscos;

II. Sensibilidade e criticidade das Informações: Criticidade dos maiores riscos encontrados durante avaliação de riscos.

5.2.2. NÍVEIS DE CONFIDENCIALIDADE

Para a realização da classificação devem ser considerados quatro aspectos importantes, os quais devem servir como fundamento. São eles:

I. **Integridade**: informação atualizada, completa e mantida por pessoal autorizado;

II. **Disponibilidade**: informação constante e sempre que necessário para pessoal autorizado;

III. **Valor**: a informação deve ter um valor agregado para o **TIC do STPP/RMC**;

IV. **Confidencialidade**: Acesso exclusivo por pessoal autorizado.

Todas as informações devem ser classificadas de acordo com os níveis de confidencialidade abaixo:

NÍVEL DE CONFIDENCIALIDADE	RÓTULOS	CRITÉRIOS DE CLASSIFICAÇÃO	RESTRIÇÃO DE ACESSOS
Público	Público	Todos podem ter acesso.	Nenhum
Confidencial	Confidencial	Possui informações uteis a atacantes, somente as pessoas envolvidas no projeto podem ter acesso às informações.	Somente os envolvidos no projeto podem ter acesso às informações.
Interno	Interno	Informações individuais de cada ente envolvido na operação como Agente de TIC do STPP/RMC.	Somente pessoas das organizações devem ter a acesso a sua própria informação restrita.

Por padrão as informações transitadas com dados do **TIC do STPP/RMC** devem circular com a classificação confidencial, garantindo um nível adequado de proteção, ainda deve ser assegurado a utilização de controles criptográficos.

AGÊNCIA DE ASSUNTOS METROPOLITANOS DO PARANÁ – AMEP
Palácio das Araucárias – Rua Jacy Loureiro de Campos, s/n – 1º andar – Centro Cívico – CEP 80.530-140 – Curitiba – Paraná
(41) 3320 6900 I www.amep.pr.gov.br

5.2.3. RECLASSIFICAÇÃO

Os proprietários de ativos devem analisar o nível de confidencialidade de seus ativos de informações e avaliar se o nível de confidencialidade pode ser mantido ou alterado. Se possível, o nível de confidencialidade deve ser reduzido (mais restrito).

5.2.4. IDENTIFICAÇÃO DA CLASSIFICAÇÃO

Forma de identificação da classificação da informação em cada meio. Vale ressaltar que essa identificação será obrigatória apenas para as informações de níveis restrito e sigiloso.

TIPO DE DOCUMENTO	PROCEDIMENTO
Papel	Para documentos gerados com dados do TIC do STPP/RMC a identificação deverá ser feita no cabeçalho de todas as páginas, inclusive na capa. Para documentos externos recebidos, deverá ser marcado com uma etiqueta na parte superior.
E-mail	A identificação deverá ser identificada no assunto do e-mail.
Documentos eletrônicos	A identificação deve ser feita utilizando rótulos.
Dados e aplicações	Deve conter o nível de segurança na “meta data” do documento. Para qualquer relatório gerado a identificação deverá ser descrita no cabeçalho.
Outros Tipos	A classificação deverá estar visível no início do documento.

5.2.5. ARMAZENAMENTO E TRAMITAÇÃO

O armazenamento e tramitação de documentos eletrônicos são controlados pelos proprietários. Ainda, no que se referem documentos impressos:

GRAU DE SIGILO	FORMA DE ARMAZENAMENTO	FORMA DE TRAMITAÇÃO
Público	Sem requisitos específicos	Sem requisitos específicos
Confidencial	Armazenamento em local seguro com acesso restrito.	Envelope lacrado, com identificação de informação “Confidencial” e confirmação de recebimento.
Interno	Armazenamento em local seguro com acesso restrito.	Envelope lacrado, com identificação de informação interna e confirmação de recebimento.

5.2.6. DESCARTE DA INFORMAÇÃO

I. No meio eletrônico, as informações devem ser deletadas permanentemente onde estiverem armazenadas;

II. No meio impresso todo documento com informações relevantes deve ser destruído antes de descartadas, podendo ser utilizado picotadores de papel.

Descarte de Mídias Físicas (Reutilização/Alienação/Descarte de equipamentos):

III. Todo equipamento antes de ser relocado/reutilizado/descartado deverá obrigatoriamente passar por limpeza completa do equipamento com software adequado, que elimine qualquer forma de recuperação de informações;

IV. **Reutilização**: Antes de realizar a formatação e limpeza dos ativos e liberá-los para um novo usuário, o setor de tecnologia deve realizar uma varredura e backup dos dados armazenados por segurança. Feita a averiguação poderá seguir com o procedimento de reutilização do dispositivo;

V. **Devolução e retirada de materiais terceiros**: todas as partes envolvidas deverão ser comunicadas e assinado um termo de devolução/retirada do equipamento, previamente cabe a área de Tecnologia da Informação de cada organização garantir que o equipamento em questão não contenha informações confidenciais que possam vazar com a utilização de softwares de recuperação de dados apagados;

VI. **Disco Defeituoso**: devem ser realizadas tentativas de recuperação do disco com softwares próprios, mas se não for possível este dispositivo precisa seguir para total destruição do equipamento e descarte;

VII. **Descarte**: Para descarte de dispositivos de armazenamento de dados, como o disco rígido (HD), CDs, deve ser utilizado software com função de deixar a mídia no estado original, impedindo a recuperação de dados. Após a utilização do software o disco deve ser encaminhado para a destruição de materiais e perfurado para garantir a total destruição da mídia.

5.2.7. EXCEÇÕES

AGÊNCIA DE ASSUNTOS METROPOLITANOS DO PARANÁ – AMEP
Palácio das Araucárias – Rua Jacy Loureiro de Campos, s/n – 1º andar – Centro Cívico – CEP 80.530-140 – Curitiba – Paraná
(41) 3320 6900 I www.amep.pr.gov.br

O uso de alguns sistemas não permite a rotulação da informação, mas deverão sofrer o tratamento adequado.

5.2.8. TRANSFERÊNCIA DE INFORMAÇÕES

I. Os **Agentes de TIC do STPP/RMC** devem garantir que a comunicação e a transferência de informações sensíveis, serão realizadas através de canal seguro e que possuirá gestão de acessos a dados;

II. São estabelecidos acordos para transferência de informações através do Contrato e assinatura de acordo de confidencialidade.

AGÊNCIA DE ASSUNTOS METROPOLITANOS DO PARANÁ – AMEP
Palácio das Araucárias – Rua Jacy Loureiro de Campos, s/n – 1º andar – Centro Cívico – CEP 80.530-140 – Curitiba – Paraná
(41) 3320 6900 I www.amep.pr.gov.br

PROCEDIMENTO DE SENHAS

1. OBJETIVO

Definir sistemática para estabelecimento, atualização e controle das senhas utilizadas no **TIC do STPP/RMC**.

2. RESPONSABILIDADES

2.1. DOS AGENTES DE TIC DO STPP/RMC

I. Devem cumprir a **Política de Governança de Dados e Segurança** e assegurar que os perfis de acesso constantes no Controle de Acesso sejam seguidos;

II. Assegurar a utilização padrão de senhas seguras nas operações de **TIC do STPP/RMC**;

III. Assegurar a atualização e controle de acesso dos usuários da operação;

IV. Garantir as devidas liberações, restrições e retiradas de acesso;

V. Garantir a padronização e utilização de senhas fortes nas senhas da operação;

VI. Assegurar ferramentas que possibilitem a realização de auditorias no controle de acessos.

3. PROCEDIMENTO

3.1. DIRETRIZES DO USO DE SENHAS (REGRAS PARA CRIAÇÃO DE LOGINS E SENHAS)

I. Os **Agentes de TIC do STPP/RMC** devem garantir o gerenciamento de permissões e recursos de acesso aos serviços de rede de forma que permita a auditoria e quando possível, integração entre os sistemas;

II. Garantir que o processo de criação de logins e senhas para um novo usuário, seja realizado através de uma solicitação formal contendo, pelo menos, o nome completo do usuário e a área de trabalho;

III. Garantir periodicamente, a revisão dos acessos através de uma relação dos usuários que tiveram seu login, senha e perfil de acesso autorizado por eles. Os Gestores devem confirmar a informação, alterá-la caso seja necessário ou revogar

AGÊNCIA DE ASSUNTOS METROPOLITANOS DO PARANÁ – AMEP
Palácio das Araucárias – Rua Jacy Loureiro de Campos, s/n – 1º andar – Centro Cívico – CEP 80.530-140 – Curitiba – Paraná
(41) 3320 6900 I www.amep.pr.gov.br

o login.

3.2. PERFIL DE ACESSO DOS USUÁRIOS

I. Os **Agentes de TIC do STPP/RMC** devem assegurar que cada usuário possui um perfil de acesso à rede de dados com indicação dos diretórios, grupos, aplicativos, funcionalidades e suas permissões de direito;

II. Assegurar que aos sistemas, cada usuário deve possuir os perfis necessários para o desempenho de suas funções operacionais no **TIC do STPP/RMC**;

III. Sempre que necessário, deve ser estabelecido o mesmo perfil de acesso para um grupo de usuários;

IV. A permissão de acesso aos ativos de informação do **TIC do STPP/RMC** deve ser solicitada formalmente conforme procedimento para liberação de acesso lógico.

3.3. SENHAS DE USO NORMAL (NÃO ADMINISTRATIVAS)

Os **Agentes de TIC do STPP/RMC** devem assegurar que o usuário é o responsável exclusivo pelo uso de suas credenciais de acesso, considerando que a senha é a principal ferramenta de autenticação, ela deve ser individual, intransferível e mantida em segredo, sendo o usuário responsabilizado por qualquer transação efetuada durante o seu uso.

Garantir que as senhas não devem ser trafegadas em mensagens de e-mail, Whatsapp ou em outros formulários de uso de comunicação eletrônica, a não ser a primeira senha criada, que deverá ser alterada obrigatoriamente pelo usuário no primeiro acesso.

Os sistemas, serviços e dispositivos do ambiente tecnológico devem ser configurados para que os padrões mínimos de senha sejam exigidos na criação, conforme as recomendações de senha forte:

I. Tenham no mínimo 8 (oito) caracteres;

II. Tenham caracteres numéricos, alfabéticos e especiais.

III. Ex: {1,2,3, A, B, C, @, #, $, %, (, +};

IV. Não deve haver repetição de letras ou números na definição da senha, ou senha com 3 ou mais caracteres iguais sequenciados. Ex:(33fffggggGGG);

V. Recomendado não usar informações pessoais publicas conhecidas como, Nome,

AGÊNCIA DE ASSUNTOS METROPOLITANOS DO PARANÁ – AMEP
Palácio das Araucárias – Rua Jacy Loureiro de Campos, s/n – 1º andar – Centro Cívico – CEP 80.530-140 – Curitiba – Paraná
(41) 3320 6900 I www.amep.pr.gov.br

Data de Nascimento, RG, CPF, nome de familiares, entre outros;

VI. As senhas deverão ser substituídas, no máximo, a cada 180 (cento e oitenta) dias de utilização. Na substituição, os sistemas não devem aceitar o reuso da última senha utilizada;

VII. As digitações das senhas devem ser mascaradas na tela, armazenadas e trafegadas de forma criptografada, pelo sistema ou aplicação.

VIII. Estabelecer regras de bloqueio para seus sistemas internos como AD, Microsoft entre outros, delimitando as tentativas errôneas e o tempo ou critério para reestabelecimento da função.

IX. Devem garantir que as solicitações de acesso, além do previsto no Controle de Acesso, devem ser realizadas através de ferramenta de chamados e autorizadas pelo gestor imediato.

X. As solicitações de recuperação de senhas, por esquecimento ou outro motivo, devem ser realizadas através da ferramenta de chamados e seguirão um procedimento de validação de informações do usuário para disponibilizar as senhas iniciais.

XI. As senhas iniciais devem ser fornecidas diretamente aos usuários e configuradas de forma que, no primeiro acesso, a solicitação de troca ocorra automaticamente e que haja a obrigatoriedade da troca da primeira senha configurada. Quando possível expirar a senha dentro de um período máximo de 48h.

3.4. SENHAS DE USO PRIVILEGIADO

Os **Agentes de TIC do STPP/RMC** devem garantir que contas privilegiadas (ex: administrador, sa, root, entre outros) tenham suas as senhas trocadas frequentemente. Com exceção das contas de serviços privilegiadas.

Todas as contas privilegiadas devem estar devidamente documentadas e atreladas ao sistema e ou serviço onde estão sendo usadas. Esta informação deve ser armazenada em local seguro com restrição de perfil de acesso.

AGÊNCIA DE ASSUNTOS METROPOLITANOS DO PARANÁ – AMEP
Palácio das Araucárias – Rua Jacy Loureiro de Campos, s/n – 1º andar – Centro Cívico – CEP 80.530-140 – Curitiba – Paraná
(41) 3320 6900 I www.amep.pr.gov.br

Os acessos privilegiados, por questões de segurança, devem ser realizados por uma quantidade mínima de usuários, que terão perfis de administradores e autorização de acesso para essas funcionalidades.

Caso as contas privilegiadas não possam ter as senhas trocadas ou renomeadas, serão desabilitadas e consideradas "contas de serviço" não sendo utilizadas para qualquer tipo de acesso.

As senhas não devem ser introduzidas em linhas de comando (códigos fontes) abertas, mas, caso seja necessário, devem ser criptografadas e consideradas "contas de serviço".

3.5. BOAS PRÁTICAS PARA CRIAÇÃO DE SENHAS

Evitar a utilização de:

I. Nomes, sobrenomes, nomes de contas de usuários e dados de membros da família;

II. Números de documentos ou de telefone (ex.: 121521487-63, 988356215);

III. Placa de carros (ex.: REC1805);

IV. Datas de aniversários, festivas, ex.: (16/05/2016, 25/12/2016);

V. Sequência do teclado (ex.: asdfg123, asdfg2023, SBE2024);

VI. Palavras do dicionário (ex.: Paralelepípedo);

VII. Nomes de times de futebol, de música, de produtos, de personagens de filmes (ex.: Garota de Ipanema, GGTISee, Mickey, Mcdonalds, SBE).

Recomendável:

I. Números aleatórios;

II. Vários e diferentes tipos de caracteres;

III. Caracteres especiais;

IV. Substituir uma letra por número com semelhança visual;

V. Frase longa com letras e números.

AGÊNCIA DE ASSUNTOS METROPOLITANOS DO PARANÁ – AMEP
Palácio das Araucárias – Rua Jacy Loureiro de Campos, s/n – 1º andar – Centro Cívico – CEP 80.530-140 – Curitiba – Paraná
(41) 3320 6900 I www.amep.pr.gov.br

4. AUDITORIA DE SENHAS

Os **Agentes de TIC do STPP/RMC** devem assegurar que no período de auditoria técnica, a utilização de técnicas e ferramentas para tentar realizar a quebra de senha seja possível, desde que o sistema permita que as senhas sejam exportadas.
Garantir via ferramenta auditoria no controle de acessos.

5. MULTI FACTOR AUTHENTICATOR (MFA)

Os **Agentes de TIC do STPP/RMC** devem sempre que o sistema suportar, configurar o segundo fator de autenticação nas aplicações.

6. EXCLUSÃO DE USUÁRIO

Os **Agentes de TIC do STPP/RMC** devem garantir que quando houver desligamento de colaboradores ou terceiros, será formalizado para que as devidas exclusões de acesso sejam realizadas imediatamente;
Devem garantir que a área de tecnologia de cada organização participante, realize os procedimentos para exclusão do usuário e atualize a relação de usuários no controle de acessos;

7. BLOQUEIO DE USUÁRIO

Os **Agentes de TIC do STPP/RMC** devem garantir que quando houver afastamento por motivos de saúde de colaboradores ou terceiros da operação deve ser formalizado e solicitado para que os devidos bloqueios de acesso sejam realizados;

Devem assegurar que serão realizados os procedimentos para bloqueio do usuário e atualização da relação de usuários no controle de acessos.

8. USO DE CONTROLES CRIPTOGRÁFICOS

Os agentes devem assegurar a utilização de controles criptográficos para proteção dos arquivos, chaves de acesso em serviços de nuvem, computadores, periféricos (HD) e chaves privadas dos portais (Site).

AGÊNCIA DE ASSUNTOS METROPOLITANOS DO PARANÁ – AMEP
Palácio das Araucárias – Rua Jacy Loureiro de Campos, s/n – 1º andar – Centro Cívico – CEP 80.530-140 – Curitiba – Paraná
(41) 3320 6900 I www.amep.pr.gov.br

Classificação da informação, para notebook uso de senha (bitlocker) onde é realizado um cadastro de senha padrão, com a orientação ao usuário de troca de senha.

8.1. CONTROLES DE CHAVES CRIPTOGRÁFICAS

As chaves criptográficas que têm pertinência como autenticação de colaboradores ex.: rede interna, computadores, e-cpf, ficam sob controle dos usuários.

8.2. REQUISITOS MÍNIMOS

Toda e qualquer remessa (upload/envio) ou recebimento (download/recepção) de dados pessoais, dados pessoais sensíveis, segredos/regras de negócio ou informações classificadas como restritas ou confidencias deverá, obrigatoriamente, utilizar mecanismos de criptografia robustos, tanto para dados em trânsito quanto para dados em repouso.

O canal de comunicação utilizado para a transferência de dados com terceiros (sejam eles parceiros, fornecedores, órgãos reguladores ou clientes) deve ser protegido por protocolos de transporte seguros.

É obrigatória a adoção do protocolo TLS (*Transport Layer Security*) na versão 1.2 ou superior (preferencialmente TLS 1.3), com a desativação explícita de versões obsoletas (SSLv3, TLS 1.0 e TLS 1.1). Os algoritmos de troca de chaves devem garantir o *Forward Secrecy* (Sigilo de Encaminhamento Perfeito).

Para remessas automatizadas ou manuais de volumes de dados, deverão ser utilizados protocolos seguros como SFTP (*Secure File Transfer Protocol*) ou HTTPS. O uso de FTP convencional (sem criptografia) é expressamente proibido.

Caso o canal de transmissão não seja isolado ou a sensibilidade dos dados exija dupla camada de proteção, os arquivos deverão ser criptografados na origem (antes do envio) utilizando algoritmos de chave simétrica padrão de mercado.

Recomenda-se o uso do algoritmo AES (*Advanced Encryption Standard*) com chaves de, no mínimo, 256 bits (AES-256).

As remessas devem utilizar funções de dispersão (*hashing*) seguras, preferencialmente da família SHA-2 (*Secure Hash Algorithm 2*), como o SHA-256, para verificação da

AGÊNCIA DE ASSUNTOS METROPOLITANOS DO PARANÁ – AMEP
Palácio das Araucárias – Rua Jacy Loureiro de Campos, s/n – 1º andar – Centro Cívico – CEP 80.530-140 – Curitiba – Paraná
(41) 3320 6900 I www.amep.pr.gov.br

integridade do arquivo recebido ou enviado, mitigando riscos de alteração maliciosa no percurso (ataques de *Man-in-the-Middle*).

A segurança da criptografia depende diretamente do controle sobre as chaves de acesso. As chaves de criptografia e as senhas de abertura de arquivos nunca devem ser trafegadas pelo mesmo canal de comunicação que o arquivo de dados. Se o arquivo for enviado por SFTP/E-mail, a senha ou chave deve ser compartilhada por um segundo canal de comunicação out-of-band (ex: aplicativo de mensagem corporativo seguro, SMS ou cofre de senhas).

Todas as operações de remessa e recebimento de dados devem gerar trilhas de auditoria (logs) automatizadas, contendo a identificação do usuário ou sistema originador, carimbo de data/hora (t*imestamp*) sincronizado, volume de dados trafegado, IP de origem/destino e o status de sucesso ou falha da operação, preservando o sigilo do conteúdo dos dados trafegados.

AGÊNCIA DE ASSUNTOS METROPOLITANOS DO PARANÁ – AMEP
Palácio das Araucárias – Rua Jacy Loureiro de Campos, s/n – 1º andar – Centro Cívico – CEP 80.530-140 – Curitiba – Paraná
(41) 3320 6900 I www.amep.pr.gov.br

PROGRAMA DE INTEGRIDADE

1. OBJETIVO

1.1. O **PROGRAMA DE INTEGRIDADE** consiste, no conjunto de mecanismos e procedimentos internos de integridade, auditoria, controle e incentivo à denúncia de irregularidade e na aplicação efetiva de códigos de ética e de conduta, políticas e diretrizes com o objetivo de detectar e sanar desvios, fraudes, irregularidades e atos ilícitos praticados contra a administração pública.

1.2. O **PROGRAMA DE INTEGRIDADE** deve ser estruturado, aplicado e atualizado de acordo com as características e riscos atuais das atividades de cada pessoa jurídica, a qual, por sua vez, deve garantir o constante aprimoramento e adaptação do referido programa, visando garantir a sua efetividade.

1.3. O PROGRAMA DE INTEGRIDADE deverá ser submetido/apresentado à **CONTRATANTE** no prazo limite do **CONTRATO**, sob pena de aplicação de penalidade, nos termos previstos no **CONTRATO** e **EDITAL**, vide art. 533 do Decreto n° 10.086, de 17 de janeiro de 2022.

1.4. O **PROGRAMA DE INTEGRIDADE** implantado ou a ser implantado deverá atender ao contido no Regulamento descrito no art. 532 e seguintes do Decreto n° 10.086/2022, no que couber.

2. REGRAMENTO PARA ELABORAÇÃO DO PROGRAMA DE INTEGRIDADE

2.1. Para participar do presente certame, a **LICITANTE** deverá se comprometer (condição obrigatória) a implementar e manter o **PROGRAMA DE INTEGRIDADE OU COMPLIANCE** como objetivo institucional.

2.2.A **LICITANTE** deverá, como condição para assinatura do **CONTRATO**, apresentar declaração informando a existência de **PROGRAMA DE INTEGRIDADE OU COMPLIANCE** implantado, se este já existir.

AGÊNCIA DE ASSUNTOS METROPOLITANOS DO PARANÁ – AMEP
Palácio das Araucárias – Rua Jacy Loureiro de Campos, s/n – 1º andar – Centro Cívico – CEP 80.530-140 – Curitiba – Paraná
(41) 3320 6900 I www.amep.pr.gov.br

2.2.1. Caso a **LICITANTE** vencedora ainda não possua implantado **PROGRAMA DE INTEGRIDADE OU COMPLIANCE**, deverá apresentar declaração se comprometendo a implantá-lo, no de até 6 (seis) meses, a contar da assinatura do **CONTRATO**, sob de pena de aplicação das penalidades previstas no **EDITAL** e na legislação.

DISPOSIÇÕES FINAIS

Esta **Política de Governança de Dados e Segurança**, bem como qualquer outra política que verse sobre Tecnologia da Informação ou Dados de **STPP/RMC**, será objeto de revisão no prazo mínimo de 4 (quatro) anos, nos mesmos termos das definições para fins de revisão ordinária da política tarifária, podendo ser revisada em prazo inferior a qualquer momento desde que para fins de atendimento ao interesse público.

Curitiba/PR, datado e assinado eletronicamente.

Elaborado por:

COMISSÃO DE CONTRATAÇÃO ESPECIAL

DESIGNADA PELA PORTARIA/AMEP N° 44/2025

AGÊNCIA DE ASSUNTOS METROPOLITANOS DO PARANÁ – AMEP
Palácio das Araucárias – Rua Jacy Loureiro de Campos, s/n – 1º andar – Centro Cívico – CEP 80.530-140 – Curitiba – Paraná
(41) 3320 6900 I www.amep.pr.gov.br

Documento: **11.ANEXOXIPOLITICADEGOVERNANCADEDADOSESEGURANCA.pdf**.

Assinatura Avançada realizada por: **Claudio Jose Zerbeto Assis (XXX.650.659-XX)** em 01/07/2026 18:13 Local: AMEP/DTIM, **Joacir da Silva Rodrigues (XXX.303.389-XX)** em 01/07/2026 18:15 Local: AMEP/CLSTPP, **Jose Guilherme Sikorski Van Der Neut (XXX.706.969-XX)** em 01/07/2026 18:16 Local: AMEP/DTIM, **Lucas Humaita Blitzkow da Silva (XXX.041.069-XX)** em 01/07/2026 18:16 Local: AMEP/DTIM, **Wilianson Correa (XXX.029.209-XX)** em 01/07/2026 18:17 Local: AMEP/DTIM, **Ana Silvia Smania Gomes (XXX.971.158-XX)** em 01/07/2026 18:18 Local: AMEP/DTIM, **Almir Nunes de Faria (XXX.847.489-XX)** em 01/07/2026 18:25 Local: AMEP/DTIM, **Wilhelm Eduard Milward de Azevedo Meiners (XXX.667.189-XX)** em 01/07/2026 18:27 Local: AMEP/DTIM, **Marlon Szymanski Betin (XXX.616.849-XX)** em 01/07/2026 18:34 Local: AMEP/DTIM.

Inserido ao protocolo **25.697.526-2** por: **Joacir da Silva Rodrigues** em: 01/07/2026 17:58.