1. INTRODUÇÃO

As informações tratadas pela São Paulo Transporte S/A, a seguir denominada SPTrans e Empresa, são ativos valiosos para a eficiente prestação de serviços públicos à sociedade. Nesse sentido, a segurança é aspecto essencial para a adequada gestão das informações sob sua custódia, que tem o dever de protegê-las.

No âmbito interno da SPTrans, de suas relações institucionais e ainda de suas relações com a sociedade, há a necessidade de orientar a condução de ações estratégicas em Segurança da Informação e o estabelecimento de normas, definindo os requisitos e metodologias para implantação da Gestão de Segurança da Informação.

Dessa forma, como as práticas de segurança da informação extrapolam aquelas relacionadas à tecnologia, pois envolvem também pessoas, processos e ambiente, foi criado um grupo específico para tratar do tema, o Comitê de Segurança da Informação – CSI. Dentre outras atribuições, este colegiado deve aprovar as diretrizes, políticas e normas gerais e específicas para as atividades relacionadas à segurança da informação no âmbito da SPTrans e de suas relações externas, assim como dirimir possíveis conflitos em relação a outras normas, códigos e procedimentos já instituídos.

É fundamental também para a Empresa que a Política de Segurança da Informação – PSI, como instrumento vestibular do arcabouço normativo da segurança da informação na SPTrans, forneça princípios, diretrizes, critérios, suporte técnico e administrativo, competências, responsabilidades e disposições gerais suficientes à implementação de práticas relacionadas à segurança da informação e comunicação.

Ademais, cabe às áreas da SPTrans a contínua identificação de processos relevantes e de caráter prioritário sob a ótica da melhoria de procedimentos administrativos e técnicos, fortalecimento dos controles internos, segurança da informação, análise e prevenção de riscos e fraudes.

2. OBJETIVOS

2.1. Estabelecer os princípios e diretrizes estratégicas de um modelo de Gestão da Segurança da Informação, por meio da implantação de controles para uso seguro, ético e legal das informações, dos ativos intangíveis e dos recursos de Tecnologia da Informação e Comunicação – TIC no âmbito da SPTrans.

2.2. Declarar formalmente o compromisso da SPTrans com a proteção das informações, dos ativos intangíveis e dos recursos de TIC de sua propriedade ou sob a sua guarda, devendo ser cumprida por todos os seus usuários.

2.3. Promover e motivar a criação e manutenção de uma cultura de Segurança da Informação, abrangendo todos os seus usuários na execução de suas atividades profissionais, bem como seus processos de trabalho, buscando o envolvimento de todas as Diretorias e Áreas da Empresa.

2.4. Zelar pela preservação dos cinco atributos fundamentais da Segurança da Informação:

a. Autenticidade

Garantir que a informação é procedente e fidedigna, capaz de gerar evidências não repudiáveis da identificação de quem a criou, editou ou emitiu.

b. Confidencialidade

Garantir que as informações restritas e sigilosas sejam acessadas e reveladas somente a indivíduos, entidades e processos devidamente autorizados.

c. Disponibilidade

Garantir que as informações e recursos de TIC estejam disponíveis sempre que necessário e mediante a devida autorização para seu acesso ou uso.

d. Integridade

Garantir que as informações estejam protegidas contra manipulações e alterações indevidas.

e. Legalidade

Garantir que todas as informações sejam criadas e gerenciadas de acordo a legislação em vigor.

2.5. Zelar, sem prejuízo de outros, pelos atributos complementares da Segurança da Informação:

a. Irretratabilidade

Garantir a capacidade de provar a ocorrência e determinado evento ou ação, bem como provar a sua autoria ou responsabilidade.

b. Rastreabilidade

Garantir a capacidade de detectar a ocorrência de determinado evento ou ação, prover caracterização adequada do fato e determinar a sua autoria.

c. Confiabilidade
Garantir a propriedade de obter comportamentos e resultados de forma prevista e consistente.

d. Utilidade

Garantir a propriedade de agregar ou gerar valor em termos organizacionais.

e. Consciência

Garantir que o tratamento da informação tenha valor relevante em termos pessoais e organizacionais.

2.6. Possibilitar a criação de controles e promover a otimização dos recursos e investimentos em Tecnologia da Informação e Comunicação – TIC, contribuindo com a minimização dos riscos associados.

3. BASE LEGAL E NORMATIVA

- Constituição da República Federativa do Brasil de 1988;
- Lei Federal nº 12.965 (Marco Civil da Internet), de 23.04.2014, a qual estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil;
- Lei nº 13.303, de 30.06.2016, a qual dispõe sobre o estatuto jurídico da empresa pública, da sociedade de economia mista e de suas subsidiárias, no âmbito da União, dos Estados, do Distrito Federal e dos Municípios;
- Decreto Municipal nº 57.653, de 07.04.2017, o qual dispõe sobre a Política Municipal de Governança de Tecnologia da Informação e Comunicação – PMGTIC, no âmbito da Administração Pública Municipal, e alterações;
- Decreto Municipal nº 49.914, de 14.08.2008, que dispõe sobre a proibição de acesso a sites da Internet com conteúdos relacionados a sexo, drogas, pornografia, pedofilia, violência e armamento, no âmbito dos órgãos integrantes da Administração Municipal Direta e Indireta;
- Código de Conduta e Integridade da SPTrans;
- Lei Federal nº 13.709 (Lei Geral de Proteção de Dados Pessoais), de 14.08.2018, a qual dispõe sobre a proteção de dados pessoais, cria a Autoridade Nacional de Proteção de Dados e dá outras providências;
- Lei Federal nº 13.853, de 08.07.2019, a qual altera a Lei Federal nº 13.709;
- Lei Federal nº 10.406, de 10/01/2002 - Código Civil;
- Lei Federal nº 13.105, de 16/03/2015 - Código de Processo Civil;
- Decreto-Lei nº 2.848, de 7/12/1940 - Código Penal;
- Decreto-Lei nº 3.689, de 3/10/1941 - Código de Processo Penal;
- Lei Federal nº 8.078, de 11/09/1990 – Código de Defesa do Consumidor;
- Decreto-Lei nº 4.657, de 04/09/1942 – Lei de Introdução às Normas do Direito Brasileiro;
- Lei Federal nº 5.172, de 25/10/1966 - Código Tributário Nacional;
- Lei Federal nº 9.610, de 19/02/1998 – Legislação sobre direitos autorais;

- Lei Federal nº 9.279, de 14/05/1996 - Direitos e obrigações relativos à propriedade industrial;
- Lei Federal nº 9.609, de 19/02/1998 - Proteção da propriedade intelectual de programa de computador;
- Lei Federal nº 8.069 de 13/07/1990 – Estatuto da Criança e do Adolescente;
- Lei Federal nº 9.296, de 24/07/1996 - Lei de Interceptação Telefônica;
- Lei Federal nº 12.735, de 30/11/2012 – Legislação sobre Crimes Digitais (Tipificação das condutas realizadas mediante uso de sistema eletrônico digital ou similares);
- Lei Federal nº 12.737, de 30/11/2012 – Legislação sobre Crimes Digitais (Tipificação de delitos informáticos);
- Lei Federal n° 12.527, de 18/11/2011 - Regula o acesso a informações previsto no inciso XXXIII do artigo 5º, no inciso II do § 3º do artigo 37 e no § 2º do artigo 216 da Constituição Federal;
- Decreto nº 8.771, de 11/05/2016 – Regulamenta a Lei 12.965, de 23/04/2014 – Marco Civil da Internet;
- NBR-ISO 31000 – Gestão de Riscos – Princípios e Diretrizes;
- COBIT 5 – Control Objectives for Information and Related Technology. ISACA, ITGI, 2007.

Este documento considera as boas práticas preconizadas pelas normas ABNT NBR ISO/IEC 27001:2013, 27002:2013, 27003:2011 e 27005:2011 em segurança da informação, assim como as legislações governamentais.

4. AMPLITUDE

Aplica-se a todos os empregados, Diretores, membros dos Conselhos de Administração e Fiscal, membros dos Comitês Estatutários, menores aprendizes, estagiários e prestadores de serviço, assim como qualquer pessoa que utilize ou venha a ter acesso às informações e recursos de TIC da SPTrans.

5. DEFINIÇÕES

5.1. Agentes de Tratamento de Dados

Trata-se de duas entidades distintas sendo: o Operador e o Controlador.

5.2. Ameaça

É a causa potencial de um incidente indesejado, da qual está sujeito resultar dano à SPTrans ou exposição indevida da informação.

5.3. Análise de Riscos

É o uso sistemático de informações para identificar fontes e estimar o risco.

5.4. Anonimização

É a utilização de meio técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta a um indivíduo.

5.5. Aplicativo P2P

É uma rede de computadores denominada *peer-to-peer*, que compartilham arquivos em uma rede, interna ou externa, sem um servidor geral que os armazene, mas usuários que ao mesmo tempo fazem download e os disponibilizam para que outros busquem arquivos em sua máquina.

5.6. Ativo

É qualquer objeto, item ou produto que tenha valor para a organização.

5.7. Ativo de Informação

É a base de dados e arquivos, contratos e acordos, documentação de sistema, informações sobre pesquisa, manuais de usuário, material de treinamento, procedimentos de suporte ou operação, planos de continuidade do negócio, procedimentos de recuperação, trilhas de auditoria e informações armazenadas.

5.8. Ativo Intangível

É o elemento que possui valor para a SPTrans e que esteja em suporte digital ou constitua-se de forma abstrata, mas registrável ou perceptível, tais como reputação, imagem, marca e conhecimento.

5.9. Classificação da Informação

É a identificação de quais são os níveis de proteção que a Informação demanda e estabelecimento de categorias e formas de identificá-las, além de determinar os controles necessários a cada uma.

5.10. Competência

É o poder ou autoridade passível de ser aplicado para a consecução de determinados atos, decisões, atividades.

5.11. Confidencialidade

É a propriedade de a informação não estar disponível ou não ser revelada para usuários ou terceiros não autorizados.

5.12. Conformidade

É o dever de cumprir, de estar em concordância e fazer cumprir regulamentos internos e externos impostos às atividades da SPTrans.

5.13. Continuidade do Negócio

É a capacidade da organização de continuar a entregar produtos ou serviços, em um nível aceitável previamente definido, após incidentes que causem sua interrupção.

5.14. Controlador

É a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

5.15. Controle

Todo método ou ação que avalie ou altere o risco de uma informação.

5.16. Controle de Risco

É a forma de gerenciar o risco, incluindo políticas, procedimentos, diretrizes, práticas ou estruturas organizacionais, que podem ser de natureza administrativa, técnica, de gestão ou legal.

5.17. Criptografia

É o processo de escrita à base de métodos lógicos e controlados por chaves, cifras ou códigos, de forma que somente os usuários autorizados possam restabelecer sua forma original.

5.18. Custodiante da informação ou custodiante

É o usuário, grupo de trabalho ou áreas delegadas pelo proprietário do ativo de informação para cuidar da manutenção e guarda do ativo de informação no dia a dia. Geralmente, não faz parte do grupo de acesso e, portanto, não está autorizado a acessar a informação.

5.19. Dado

É a parte elementar da estrutura do conhecimento, computável, mas, incapaz de, isoladamente, gerar conclusões inteligíveis ao destinatário.

5.20. Dados Anonimizados

São, nos termos da Lei Federal nº 13.709/2018, as informações relativas aos titulares que não possam ser identificadas, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.

5.21. Dados Cadastrais

São informações identificadoras perante os cadastros de órgãos públicos, tais como os atributos biográficos, o número de inscrição no Cadastro de Pessoas Físicas (CPF), o número de inscrição no Cadastro Nacional de Pessoas Jurídicas (CNPJ), o Número de Identificação Social (NIS), o número de inscrição no Programa de Integração Social (PIS), o número de inscrição no Programa de Formação do Patrimônio do Servidor Público (PASEP), o número do Título de Eleitor, a razão social, o nome fantasia e a data de constituição da pessoa jurídica, o tipo societário, a composição societária atual e histórica e a Classificação Nacional de Atividades Econômicas (CNAE) e outros dados públicos relativos à pessoa jurídica ou à empresa individual.

5.22. Dados Pessoais

São as informações relacionadas à pessoa natural identificada ou identificável.

5.23. Dados Pessoais de Crianças e Adolescentes

São informações relacionadas a crianças de até 12 anos de idade incompletos e adolescentes, aquela entre 12 e 18 anos.

5.24. Dados Pessoais Sensíveis

São informações pessoais sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculadas a uma pessoa natural.

5.25. Dispositivo de Identificação Digital

É o recurso tecnológico que possibilita identificar e autenticar o usuário em ambientes lógicos e físicos, tais como crachá magnético, certificado digital, *token* e biometria.

5.26. Dispositivo Móvel

É o equipamento que tem como características a capacidade de registro, armazenamento ou processamento de informações, possibilidade de estabelecer conexões e interagir com outros sistemas ou redes, além de serem facilmente transportados devido a sua portabilidade, como, por exemplo, pen drives, celulares, smartphones, notebooks, desktops, tablets, equipamentos reprodutores de MP3, câmeras de fotografia ou filmagem, ou qualquer dispositivo que permita conexão à internet, portabilidade ou armazenagem de dados.

5.27. Evento de Segurança da Informação

É a ocorrência identificada de um estado de sistema, serviço ou rede, indicando uma possível violação da política de segurança da informação ou falha de controles, ou uma situação previamente desconhecida, que possa ser relevante para a segurança da informação.

5.28. Gestor da Informação

É a pessoa responsável pela informação e pela sua classificação, realizando revisões sobre os perfis de acesso dentro dos sistemas de informação da SPTrans.

5.29. Governança de Segurança da Informação

É o conjunto de princípios e processos pelo qual a SPTrans fornece visões e orientações das atividades relacionadas à Segurança da Informação.

5.30. Incidente de Segurança da Informação

É o evento ou série de eventos indesejados ou inesperados, que causem ou que tenham uma grande probabilidade de causar dano à SPTrans e ameaçar a segurança da informação.

5.31. Informação

É o conjunto de dados que, processados ou não, podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato.

5.32. Internet

É o sistema constituído do conjunto de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes.

5.33. Log

É o registro de atividades gerado por programa de computador que possibilita a reconstrução, revisão e análise das operações, procedimento ou evento em sistemas de informação.

5.34. Mídia Social

É a plataforma baseada em internet, sobre a qual ocorre a interação entre pessoas físicas ou jurídicas e a produção, troca ou compartilhamento de informações.

5.35. Operador

É a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

5.36. Perfil por Função

É o agrupamento de acesso baseado na função dos empregados, o qual visa disponibilizar todos os acessos pertinentes a determinado cargo, com as funções para que um novo colaborador possa desempenhar suas atividades.

5.37. *Phishing*

É a forma de fraude eletrônica, caracterizada por tentativas de adquirir dados pessoais, ao se fazer passar como uma pessoa confiável ou uma empresa enviando uma comunicação eletrônica oficial. Isto ocorre de várias maneiras, principalmente por e-mail, mensagem instantânea, SMS, dentre outros.

5.38. Políticas

São as intenções e diretrizes de uma organização conforme dispostas pela Alta Administração.

5.39. Privacidade

É a inviolabilidade do direito à intimidade, à vida privada, à honra e à imagem das pessoas.

5.40. Recursos de Tecnologia da Informação e Comunicação - TIC

É o conjunto de recursos físicos e lógicos utilizados para criar, armazenar, manusear, transportar, compartilhar e descartar a informação, como, por exemplo, microcomputadores, *desktops*, *notebooks*, *smartphones*, *tablets*, *pendrives*, mídias, impressoras, *scanners*, *softwares*, entre outros.

5.41. Risco

É a combinação da probabilidade da concretização de uma ameaça e seus potenciais impactos.

5.42. Segurança da Informação

É a preservação da confidencialidade, integridade e disponibilidade da informação e, ainda, de suas outras propriedades ou atributos, tais como autenticidade, responsabilidade, irretratabilidade ou não repúdio e confiabilidade.

5.43. Service Level Agreement (SLA)

É o Acordo de Nível de Serviço (ANS), que é fundamental para qualquer contrato de prestação de serviços na TI, fazendo referência à especificação, em termos mensuráveis e claros, de todos os serviços que o contratante pode esperar do fornecedor na negociação.

5.44. Security Office

É a parte integrante da Área de Tecnologia da Informação e Comunicação que realiza a gestão dos acessos concedendo ou revogando permissões em função do perfil do usuário ou ainda a necessidade de acesso, zelando pelo cumprimento da Política de Segurança da Informação estabelecida.

5.45. Senha

É o grupo de caracteres secretos que permitem o acesso aos dados, identificando quem tiver efetuado o acesso.

5.46. Serviço Corporativo

É o serviço oferecido pela SPTrans aos usuários dos recursos de TIC, por meios próprios ou por contratos com terceiros.

5.47. Software Malicioso

É o programa que, normalmente, têm duas etapas de funcionamento: a ação e a propagação. Na ação, o *software* malicioso gera o risco de mostrar mensagens, criar canais de comunicação, obter informações do computador infectado, formatar o disco rígido, embaralhar o vídeo, entre outras ações. A propagação tem por objetivo a difusão do programa.

5.48. Tecnologia da Informação e Comunicação

É um conjunto de ferramentas tecnológicas utilizadas de forma incorporada para que seja possível chegar mais rápido e intuitivamente ao seu objetivo de negócio. Também conhecido pela sigla TIC.

5.49. Titular

É a pessoa natural a quem se referem os dados pessoais que são objetos de tratamento.

5.50. Usuário

É o Diretor, empregado, estagiário, menor aprendiz, prestador de serviço, terceirizado, parceiro, convenente, conveniado, credenciado, fornecedor ou qualquer outro indivíduo ou organização que venham a ter relacionamento, diretamente, com a SPTrans.

5.51. Violação

É qualquer atividade que desrespeite as diretrizes estabelecidas nesta Política ou em quaisquer das demais normas que a complemente.

5.52. Vírus

É um programa de computador que se autoagrega a outros programas existentes no computador com o objetivo de destruir e/ou roubar informações, sendo que uma vez agregado e utilizando os recursos do programa infectado, o vírus se replica e infecta outros programas.

6. PRINCÍPIOS DE SEGURANÇA DA INFORMAÇÃO

6.1. Legalidade

Cumprimento da legislação vigente no Brasil, além dos instrumentos regulamentares relacionados às atividades profissionais e aos objetivos institucionais e éticos da Administração Pública e a observância das boas práticas de mercado sobre segurança da informação.

6.2. Defesa em Profundidade

Estratégia de segurança de informação que busca integrar pessoas, tecnologia e recursos instituindo múltiplos, redundantes e independentes níveis de proteção, considerando o valor dos ativos para a organização.

6.3. Simplicidade

Favorecimento da implementação de salvaguardas simples, suficientes e eficazes.

6.4. Proteção dos Ativos

Preservação e proteção da imagem, logotipo, reputação e demais ativos intangíveis de diversos tipos de ameaça, tais como acesso, divulgação, compartilhamento ou modificação não autorizados.

6.5. Cultura de Segurança da Informação

Incorporação e manutenção, por todos os usuários, da segurança da informação como um elemento essencial em seus hábitos e atitudes dentro e fora da organização.

6.6. Privilégio Mínimo

Concessão aos usuários apenas das permissões estritamente necessárias para a execução das atividades profissionais designadas.

6.7. Celeridade

Oferecimento de ações rápidas em resposta a incidentes e falhas, visando reduzir os impactos gerados por incidentes de segurança.

6.8. Responsabilidade

Definição clara das responsabilidades primárias e finais pela proteção de cada ativo e pelo cumprimento de processos de segurança.

6.9. Resiliência

Capacidade de a organização se adaptar e manter a continuidade de seu negócio frente a grandes mudanças e situações de crise.

6.10. Valoração da Informação

A informação possui valor para a SPTrans e, portanto, devem existir mecanismos físicos, tecnológicos, pessoais, processuais, organizacionais e normativos implementados para conferir-lhe adequado tratamento de forma a atender efetivamente aos interesses da Empresa.

6.11. Confiança

Autonomia e facilitação da atuação de pessoas ou processos automatizados que, em função do tipo do ativo, do perfil da pessoa e da criticidade da informação, sejam aderentes aos critérios e atributos de Segurança da Informação.

6.12. Extensibilidade

Extensão e a complementação da Política de Segurança da Informação – PSI por meio de normas adicionais, visando a dar adequado alcance e profundidade às normas de Segurança da Informação.

7. DIRETRIZES E CRITÉRIOS

7.1. Gerais

7.1.1. Esta Política pautar-se-á pela Política Municipal de Governança de Tecnologia da Informação e Comunicação.

7.1.2. A interpretação da Política de Segurança da Informação – PSI deverá ser realizada observando-se todos os princípios de segurança da informação expressos no item 6 do presente instrumento.

7.1.3. Todo caso de exceção às determinações da Política de Segurança da Informação – PSI deve ser analisado de forma individual, aplicável apenas ao seu solicitante, dentro dos limites e motivos que o tiverem fundamentado.

7.1.4. Todos os ativos intangíveis, recursos de TIC e informações de propriedade ou sob custódia da SPTrans deverão ter seu uso e compartilhamento oportunamente regulamentados por norma específica.

7.1.5. Cada Área da SPTrans deverá estabelecer um processo de gestão de risco de segurança da informação, com o objetivo de identificar as necessidades da organização em relação aos requisitos de segurança da informação, contemplando, no mínimo, os critérios de avaliação, de tratamento do risco e, quando for o caso, da aceitação do risco residual.

7.1.6. São de responsabilidade de cada Área as informações produzidas, acessadas, processadas e armazenadas, bem como quaisquer *softwares*, banco de dados ou conteúdos que forem criados pelos usuários, em função do cumprimento de suas atribuições ou sob solicitação e em proveito da SPTrans.

7.1.7. Os *softwares* adquiridos de terceiros e aqueles que estejam de posse da SPTrans não poderão ser copiados, salvo se houver expressa previsão nos termos de licenciamento de software e se previamente autorizado por escrito pelo titular.

7.1.8. As informações custodiadas pela SPTrans deverão ser produzidas, acessadas, processadas, armazenadas e destruídas em consonância com o disposto no item 7.5.2.1 e seguintes deste instrumento.

7.1.9. Todas as informações e recursos institucionais de TIC deverão ser tratados para o cumprimento das atribuições legais, regulamentares e estatutárias da SPTrans, dentro do padrão ético estabelecido no Código de Conduta e Integridade, preservando a classificação da informação indicada.

7.1.10. É vedada a utilização da identidade visual, logos, marcas ou quaisquer outros sinais distintivos atuais e futuros da SPTrans para fins particulares, em qualquer forma ou mídia, inclusive na internet e nas mídias sociais.

7.2. Recursos Humanos

7.2.1. A SPTrans deverá assegurar que todos os usuários tomem ciência de suas responsabilidades e atuem em consonância com esta Política e demais normas adotadas pela SPTrans para a Gestão de Segurança da Informação, para que o risco de furto ou sequestro de informações classificadas em grau restrito ou sigiloso, de fraude, de vazamento, de mau uso de informações, de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito, seja reduzido.

7.2.2. As Áreas da SPTrans deverão conscientizar constantemente seus usuários, incluindo empregados, parceiros ou convenentes e prestadores de serviços, no uso ético, seguro e legal das informações e dos recursos institucionais de TIC por ela disponibilizados ou tratados.

7.2.3. Todos os relacionamentos, parcerias, convênios e contratações em que houver o compartilhamento de informações da SPTrans ou sob a sua guarda da ou ainda a concessão de qualquer tipo de acesso aos seus ambientes e recursos de TIC deverão contar, conforme o caso, com a:

a. Celebração de Termo de Uso e Responsabilidade;
b. Celebração de Termo de Confidencialidade ou inclusão de cláusulas contratuais que tratem especificamente de segurança da informação; e
c. Declaração de ciência e aceite do Código de Conduta e Integridade e da Política de Segurança da Informação – PSI da SPTrans.

7.3. Segurança Física e do Ambiente

7.3.1. As Áreas da SPTrans deverão estabelecer mecanismos de proteção para as instalações físicas e para as áreas de tratamento das informações, alinhados aos riscos identificados, prevenindo o acesso físico não autorizado, danos ou interferências.

7.3.2. Deverão ser oportunamente elaborados normativos específicos dispondo sobre os procedimentos para acesso físico dos usuários às dependências e instalações físicas da SPTrans.

7.3.3. Todos os envolvidos em trabalhos terceirizados, tais como os de segurança patrimonial, de manutenção das instalações físicas e de serviços de conservação e limpeza, deverão ser orientados e capacitados para manter as medidas de proteção de acesso adotadas pela SPTrans.

7.3.4. Não serão permitidos registros fotográficos, de imagens, filmagens ou captura de sons no ambiente corporativo da SPTrans, salvo quando houver autorização explícita da gerência onde ocorrerem os registros.

7.3.5. São vedados a divulgação e o compartilhamento do conteúdo de que trata o item 7.3.4 em mídias sociais, internet ou outros meios eletrônicos, exceto quando forem realizados ou autorizados pela Área competente.

7.4. Gestão de Ativos

7.4.1. Inventário dos Ativos e Responsabilidade

7.4.1.1. A SPTrans deverá possuir processo estruturado de identificação e inventário de ativos.

7.4.1.2. Todos os ativos deverão possuir um responsável designado pela sua gestão.

7.4.1.3. Deverão ser adotados processos formais de inventário e identificação de recursos de TIC, de acordo com sua relevância para a instituição.

7.4.1.4. Deverão ser estabelecidos controles de segurança lógicos aplicáveis aos recursos institucionais de TIC.

7.4.2. Uso dos Recursos de Tecnologia da Informação e Comunicação

7.4.2.1. Todo recurso de TIC, quando conectado à rede da SPTrans ou utilizado para finalidade institucional, deverá possuir ferramentas de proteção contra *software* malicioso sempre ativas e atualizadas, sendo vedado ao usuário efetuar alteração de configuração, remoção ou desativação de tais ferramentas.

7.4.2.2. É vedado visualizar, acessar, baixar ou transmitir arquivos, utilizar, instalar, armazenar, divulgar ou repassar qualquer material, conteúdo, ou recurso ilícito, impróprio, obsceno, pornográfico, ofensivo, discriminatório, que atente contra os princípios éticos adotados pela Empresa, bem como que seja incompatível com as diretrizes e interesses da SPTrans, por meio de recursos de TIC conectados à rede corporativa.

7.4.2.3. O uso aceitável de recurso particular de TIC, quando conectado à rede corporativa, será oportunamente regulamentado por normativo específico.

7.4.2.4. Usuários são plenamente responsáveis pelo conteúdo que estiver armazenado em seus recursos particulares de TIC e deverão estar cientes de que a SPTrans isenta-se de qualquer responsabilidade em casos de extravio, furto, roubo ou qualquer outra circunstância que afete a detenção de posse ou integridade desses recursos trazidos às suas instalações ou que estejam conectados à rede corporativa, ainda que fora de seu perímetro físico, reservando-se ao direito de inspecionar esses recursos sem prévio aviso, se necessário.

7.4.2.5. Os processos de manutenção, instalação, configuração, desinstalação, substituição ou remanejamento dos recursos de TIC deverão ser realizados pela Área competente da SPTrans.

7.4.2.6. A SPTrans deverá monitorar, rastrear e manter o registro de todos os acessos aos serviços e sistemas informatizados realizados pelos usuários por meio da sua rede corporativa.

7.5. Gestão da Informação

7.5.1. Classificação da Informação

7.5.1.1. A classificação das informações e seu gerenciamento devem obedecer a Tabela de Temporariedade e suas classificações vigentes na SPTrans.

7.5.1.2. A classificação das informações servirá de base para determinar controles adequados para protegê-las, bem como os rótulos que serão aplicados de forma a permitir sua fácil identificação.

7.5.2. Tratamento da Informação

7.5.2.1. Cada usuário é responsável pela segurança das informações às quais tiver acesso em decorrência de suas atividades, principalmente daquelas que estiverem sob a sua tutela.

7.5.2.2. Os controles aplicáveis no gerenciamento da informação deverão levar em consideração todo o seu ciclo de vida, o qual compreende sua criação, registro, classificação, acesso, manuseio, modificação, reprodução, distribuição, delegação, compartilhamento, publicação, transmissão, armazenamento, arquivamento e destruição.

7.5.2.3. Deverão ser usados os controles de segurança apropriados para proteção da confidencialidade e integridade de informações de propriedade ou sob a responsabilidade da SPTrans que tenha classificação que exija algum nível de restrição ou de sigilo.

7.5.2.4. É vedada a transmissão e armazenamento de arquivos de qualquer conteúdo, software ou informação de propriedade ou sob a responsabilidade da SPTrans, sem a expressa autorização da gerência da área que fará a transferência, para fora do ambiente corporativo ou para qualquer plataforma de internet, tais como: repositórios digitais, e-mails ou serviços de armazenamento de arquivos de forma geral que não tenham contrato de sigilo firmado com a SPTrans. .

7.5.2.5. A transferência e o compartilhamento de informações para outras pessoas jurídicas, inclusive para órgãos e entidades governamentais, dependerão de autorização do titular das informações e deverá ser tratada oportunamente em norma específica, observada a legislação vigente.

7.5.2.6. A comunicação, reprodução, distribuição, transferência, difusão, transmissão ou recebimento de conteúdo, mensagens ou informações institucionais deverá ser realizado, exclusivamente, por meio de serviços corporativos oferecidos pela SPTrans.

7.5.2.7. É vedado ao usuário revelar, transferir, publicar, compartilhar ou divulgar quaisquer informações de propriedade ou sob a responsabilidade da SPTrans que, nos termos da legislação vigente, não forem objeto de transparência pública, o que inclui informações relacionadas às suas rotinas de trabalho, dados de fornecedores e prestadores de serviços ou demais detalhes técnico-operacionais.

Nota: excetuam-se da vedação prevista no item acima os casos de execução de atividades institucionais, observando-se nesse caso os critérios de classificação e tratamento da informação quanto à restrição ou o sigilo.

7.5.2.8. O processo de descarte das informações e dos recursos de TIC deverá seguir os procedimentos técnicos e administrativamente seguros, que impeçam a posterior recuperação indevida da informação.

7.5.2.9. Todas as modificações nos recursos de TIC devem ser realizadas de maneira controlada, conforme processos de gestão de mudanças, de configuração e de liberação definidos para identificar riscos e possíveis impactos, além de possibilitar a restauração da operação ao ambiente original em caso de incidentes não previstos.

7.6. Controle de Acessos

7.6.1. A identificação do usuário, qualquer que seja o meio e a forma de acesso à informação, é pessoal e intransferível e deverá permitir de maneira clara e inequívoca o seu reconhecimento.

7.6.2. Os usuários são responsáveis por todos os atos praticados com as suas identificações, tais como: 0 nome de usuário, senha, *logins* de acesso, certificação digital, biometria, correio eletrônico e assinatura digital.

7.6.3. Os usuários são responsáveis pela segurança e proteção de suas senhas, devendo sempre utilizar senhas seguras e alterá-las regularmente.

7.7. Monitoramento, Auditoria e Inspeção

7.7.1. Toda auditoria dos controles de segurança dos recursos institucionais de TIC deverá ser planejada e executada regularmente, com o objetivo de verificar a conformidade com a legislação vigente e com as normas e procedimentos de segurança da informação definidos nesta Política e nos demais atos normativos a ela relacionados.

7.7.2. A periodicidade das auditorias será definida em razão da criticidade do recurso de TIC, ou da informação e da sua proteção, tal qual em decorrência de novos procedimentos recomendados e da utilização de novas tecnologias.

7.7.3. As não conformidades deverão ser registradas e classificadas, devendo os casos considerados graves serem tratados prioritariamente com prazo e responsável por sua correção determinados.

7.7.4. Os procedimentos de auditoria serão oportunamente definidos em norma específica.

7.7.5. Para fins administrativos e legais, a SPTrans poderá monitorar e armazenar os dados referentes aos acessos, ao conteúdo trafegado a partir da rede corporativa e ao uso de seus ativos intangíveis, suas informações, marcas e recursos de TIC, além de seus ambientes físicos e lógicos.

7.7.6. A SPTrans poderá, mediante prévia justificativa, auditar e realizar inspeções físicas e lógicas nos dispositivos móveis, equipamentos, sistemas ou recursos de TIC que interajam com seus ambientes lógicos ou físicos, conforme disciplinado em norma específica.

7.7.7. Os registros de *logs*, e-mails, acessos a sítios de internet, histórico de navegação, endereçamento IP, condições aceitas e quaisquer outras informações relevantes devem ser armazenados de forma segura, por prazo oportunamente estabelecido em norma específica.

7.7.8. Os controles internos dos sistemas de informação não deverão ser objeto de testes de violabilidade por parte dos usuários, exceto para aqueles que possuam tal atribuição.

7.7.9. É vedada qualquer tentativa de alteração de registros de *logs*, os quais somente poderão ser acessados por profissionais autorizados na investigação ou apuração de eventos ou incidentes de segurança da informação, de cometimento de infração, ato ilícito ou descumprimento da legislação vigente, da política, norma ou procedimento interno.

7.7.10. A SPTrans deverá realizar, periodicamente, a verificação de conformidade desta Política e das demais normas e procedimentos de segurança da informação dela decorrentes com os seus objetivos institucionais e com as boas práticas de mercado sobre segurança da informação.

7.8. Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação

7.8.1. A SPTrans deverá estabelecer regras e responsabilidades para que todos os requisitos de segurança da informação estejam identificados e contratualmente acordados antes da aquisição, do desenvolvimento e da implementação de sistemas de informação.

7.8.2. O desenvolvimento, a aquisição e a manutenção de sistemas, produtos e serviços deverão atender aos requisitos de segurança para assegurar a aplicação dos controles necessários em todas as etapas dos processos e para garantir a confidencialidade, integridade, legalidade, autenticidade e disponibilidade das informações.

7.8.3. Para a garantia de aderência aos padrões de segurança e funcionalidades, todas as aquisições de *hardware* e *software* deverão ter a aprovação da Área técnica responsável.

7.9. Gestão de Incidentes de Segurança de Informação

7.9.1. Todo incidente, suspeita de incidente, ou situações que colocarem ou puderem colocar em risco a segurança da informação deverão ser imediatamente reportados à Área técnica responsável da SPTrans, que deverá registrar, identificar, analisar, classificar e providenciar o adequado tratamento ao incidente.

7.9.2. O resultado das análises dos incidentes de segurança deverá ser utilizado para a melhoria contínua desta Política, normas, procedimentos e controles de segurança da informação.

7.9.3. As responsabilidades e os procedimentos de gestão de incidentes deverão ser estabelecidos e comunicados, visando prover respostas rápidas, efetivas e ordenadas dos incidentes de segurança da informação.

7.10. A SPTrans deverá estabelecer, por meio de normativo específico, as regras que regulamentarão o processo de Gestão de Continuidade do Negócio.

8. COMPETÊNCIAS

8.1. Comitê de Segurança da Informação - CSI

8.1.1. Estabelecer a estrutura e o funcionamento do modelo de Governança da Segurança da Informação da SPTrans.

8.1.2. Implantar projetos e ações junto às Áreas Responsáveis da SPTrans e monitorar os resultados com vistas a cumprir as disposições contidas na LGPD.

8.1.3. Aprovar e acompanhar a atualização das diretrizes, políticas e normas gerais e específicas para as atividades relacionadas à segurança da informação na SPTrans.

8.1.4. Propor e implantar mecanismos para monitorar, identificar, notificar os responsáveis, incluindo o Comitê de Gestão de Riscos, Conformidade e Controle Interno – CGC, sobre ameaças e ataques que possam comprometer a imagem institucional e a segurança dos ativos de Tecnologia da Informação e Comunicação – TIC da SPTrans, visando tratar e mitigar os eventuais incidentes.

8.1.5. Zelar pelo cumprimento da Política de Segurança da Informação – PSI, garantindo sua aplicabilidade e atualização.

8.1.6. Propor atividades de conscientização, educação e capacitação em Segurança da Informação para todas as Áreas da Empresa.

8.1.7. Apoiar as Áreas Responsáveis no aprimoramento contínuo do uso dos recursos de Tecnologia da Informação e Comunicação – TIC da SPTrans.

8.2. Conselho de Administração

8.2.1. Aprovar a Política de Segurança da Informação – PSI, encaminhada pela Diretoria Executiva.

8.3. Diretoria Executiva

8.3.1. Aprovar a Política de Segurança da Informação – PSI.

8.3.2. Promover a conscientização, em todas as Áreas da Empresa, dos riscos associados com a perda da confidencialidade, integridade e disponibilidade da Segurança da Informação.

8.3.3. Aprovar os relatórios periódicos elaborados pela Área de Tecnologia da Informação e Comunicação, para posterior aprovação do Conselho de Administração.

8.3.4. Garantir recursos para o desenvolvimento, implementação e cumprimento dos procedimentos adequados ao aprimoramento da Segurança da Informação.

8.4. Responsável da Área

8.4.1. Orientar e capacitar constantemente suas equipes quanto ao uso ético, seguro e legal das informações, dos recursos de TIC e dos valores adotados pela SPTrans, instruindo-os, inclusive, a disseminar a cultura para os demais usuários.

8.4.2. Reportar imediata e formalmente aos canais competentes da SPTrans qualquer caso comprovado, passível de comprovação ou cuja suspeita seja fundamentada, de descumprimento desta Política.

8.4.3. Cooperar na investigação de incidentes de segurança relacionados às informações, recursos de TIC e usuários sob sua responsabilidade.

8.4.4. Promover e incentivar atividades de orientação, instrução e esclarecimento de dúvidas relacionadas a esta Política.

8.4.5. Propor melhorias e novos procedimentos de Segurança da Informação relacionados à sua Área, submetendo as propostas ao Comitê de Segurança da Informação – CSI.

8.4.6. Gerir, dentro dos limites da sua atuação, os controles a serem realizados em termos de Segurança da Informação e determinar, de forma subsidiária ao estabelecido nesta Política e nas normas vigentes, eventuais controles adicionais que se fizerem convenientes ou necessários para a Área.

8.4.7. Atuar de forma diligente com relação a incidentes e vulnerabilidades das Informações de sua Área ou sob sua guarda.

8.5. Gestor da Informação

8.5.1. Classificar as informações de Segurança da Informação pertinentes ao respectivo cargo.

8.5.2. Criar e manter atualizada tabela com agrupamento de informações e responsabilidades desta Política, designando os perfis de autoridade de acesso dentro dos sistemas.

8.5.3. Conceder acessos e alterações nos perfis quando solicitado.

8.6. Usuário

8.6.1. Zelar pela proteção do patrimônio, dos ativos intangíveis, da imagem e reputação da SPTrans, evitando a exposição desnecessária das informações institucionais e agir com responsabilidade no uso dos recursos e das informações.

8.6.2. Cumprir e manter-se atualizado com relação à Política e às demais normas e procedimentos relacionados, por meio do uso responsável, profissional, ético e legal dos recursos institucionais de TIC, respeitando os direitos e as permissões de uso concedidas pela SPTrans.

8.6.3. Buscar orientação do superior hierárquico imediato em caso de dúvidas relacionadas à Segurança da Informação.

8.6.4. Proteger as informações contra acesso, modificação, destruição ou divulgação não autorizados pela SPTrans.

8.6.5. Reportar imediata e formalmente qualquer caso comprovado, passível de comprovação ou cuja suspeita seja fundamentada de descumprimento desta Política, para a sua chefia por meio de canais oficiais.

8.6.6. Utilizar somente conteúdos e informações legítimos e autorizados, de acordo com os controles de acesso estabelecidos e respeitando os direitos de propriedade intelectual e industrial da SPTrans e de terceiros.

8.6.7. Zelar, em razão do cargo, da função ou em razão da legislação vigente, pelo sigilo ou restrição imposto pela classificação da informação a que tiver acesso, não podendo utilizá-lo para a obtenção de vantagens para si ou para outrem.

8.6.8. Assinar os termos que venham a ser, formalizando a ciência e o aceite da presente Política, das normas e procedimentos respectivos, bem como assumindo responsabilidade por seu fiel cumprimento.

8.6.9. Sugerir melhorias em termos de Segurança da Informação no âmbito das suas atividades, competências ou conhecimentos.

9. CONTROLE DE ACESSO AOS SISTEMAS DE INFORMAÇÃO

9.1. O processo de autenticação do acesso do usuário aos sistemas de informação da SPTrans deverá ser realizado pela combinação mínima de dois fatores:

a. Identificação do usuário; e

b. Senha.

9.2. Caberão a todos os Diretores, empregados, estagiários, menores aprendizes, parceiros, convenentes e prestadores de serviço cuidar e manter em segredo sua senha de acesso, sob pena de serem responsabilizados por qualquer uso indevido de seu *login*.

9.3. O usuário receberá, quando possível, os acessos definidos pelo Perfil por Função correspondente, baseado nas informações de Área e já aprovado previamente pelo Gestor responsável quando da definição do perfil, sem a necessidade de aprovação específica.

9.4. Havendo necessidade de acessos fora do perfil por função deverá ser solicitada a área de TIC os respectivos acessos, justificando-se sua necessidade.

9.5. Nenhum acesso será concedido a qualquer usuário sem prévia autorização por escrito.

10. USO DE SENHAS

10.1. A senha associada com o usuário compõe a identificação do login do usuário nos sistemas de informação da SPTrans, cujo uso é individual, confidencial e exclusivo, sendo vedada a sua divulgação a terceiros sob qualquer hipótese.

10.2. A senha deverá ser trocada:

a. Imediatamente no primeiro acesso do usuário ao sistema de informação;
b. Em intervalos pré-definidos pela Área de Tecnologia da Informação e Comunicação;
c. Em periodicidade menor do que a padrão nos casos em que a aplicação assim o exigir.

10.3. É permitido ao usuário, principalmente visando preservar a confidencialidade da sua senha, alterá-la a qualquer momento.

10.4. O tamanho da senha deverá ser, no mínimo, de 8 (oito) caracteres e, no máximo, de 30 (trinta) caracteres, conforme a extensão da aplicação ou do sistema.

10.5. Deverão ser configuradas senhas fortes, com a combinação de letras maiúsculas, minúsculas, números e caracteres especiais.

10.6. A senha do usuário não poderá ser uma palavra encontrada facilmente em dicionário.

10.7. Deverão existir controles nos sistemas de informação da SPTrans, por meio de um arquivo histórico de registros, para impedir a reutilização das 10 (dez) últimas senhas configuradas pelo usuário.

10.8. Nos sistemas de informação utilizados pela SPTrans, depois de atingido o período de inatividade, deverá ser requerida uma nova autenticação do usuário.

10.9. O acesso do usuário aos sistemas de informação da SPTrans será suspenso após 3 (três) tentativas inválidas, no máximo.

10.10. A conta que não for utilizada pelo usuário em um período de 90 (noventa) dias poderá será desabilitada pela SPTrans sem prévia comunicação.

10.11. A senha do usuário deverá ser mantida de forma criptografada, não sendo permitido o acesso ao arquivo de senhas.

10.12. As senhas poderão ser reativadas, mas nunca poderão ser visualizadas.

10.13. A reativação de conta suspensa ou cuja senha tenha sido esquecida ou expirada deverá ser feita pela Área de Tecnologia da Informação e Comunicação, por meio de chamado técnico.

10.14. As senhas especiais dos administradores de rede e de ambiente deverão expirar após 90 (noventa) dias, no máximo.

10.15. Em caso de desligamento do funcionário todos os acessos e senhas serão bloqueados imediatamente no ato do desligamento.

11. REVISÃO DE ACESSO

11.1. Periodicamente, a Área de Tecnologia da Informação e Comunicação enviará para os Gestores da Informação um relatório extraído dos sistemas e de aplicações com os perfis dos usuários para que possam ser revistos as permissões de acesso.

11.2. A periodicidade da revisão de acesso dependerá da criticidade do sistema de informação utilizado, sendo semestral para os sistemas críticos e sendo anual para os demais sistemas de informação da SPTrans.

11.3. Tão logo o Gestor da Informação retorne a revisão, à Área de Tecnologia da Informação e Comunicação executará as alterações solicitadas, comunicar-lhe-á e finalizará a revisão.

11.4. A validação do acesso do Gestor da Informação poderá ser feita por ele mesmo, quando não houver um superior na hierarquia da Área.

12. RECURSOS DE ADMINISTRAÇÃO DE USUÁRIOS NOS SISTEMAS

12.1. Todo acesso deverá ser iniciado pela identificação do usuário, via *software* de gerenciamento de rede local à qual o *hardware* estiver conectado. Uma vez feita a identificação, via login/senha, o usuário terá acesso aos recursos sistêmicos.

12.2. Os usuários somente poderão fazer uso dos sistemas após a sua devida identificação na rede local.

13. CUIDADOS COM A SEGURANÇA DA INFORMAÇÃO

13.1. Segurança de Equipamento - Computador

13.1.1. O ativo de tecnologia – *hardware* e *software* – deverá ser identificado em inventário de ativos, que deverá ser realizado, no mínimo, anualmente.

13.1.2. O ativo de tecnologia somente poderá ser instalado e alterado pela Área de Tecnologia da Informação e Comunicação, sendo que qualquer exceção deverá ser previamente justificada e autorizada formalmente por aquela.

13.1.3. Somente conexões aprovadas pela Área de Tecnologia da Informação e Comunicação, tais como *gateways*, *proxy* e *firewalls*, deverão ser utilizadas.

13.1.4. Não será permitido o acesso remoto aos sistemas de informação da SPTrans sem a devida autenticação do usuário, mediante identificação e senha, na rede.

13.1.5. Todo acesso aos sistemas de informação da SPTrans feito por equipamento utilizado fora das instalações físicas da Empresa, cuja utilização tenha o propósito de dar suporte às atividades institucionais, deverá estar sujeito à autorização prévia do Responsável da Área de Tecnologia da Informação e Comunicação.

13.1.6. O antivírus deverá ser mantido permanentemente atualizado pela Área Tecnologia da Informação e Comunicação e não poderá, em nenhuma hipótese, ser desligado ou inativado pelo usuário.

13.1.7. A Área de Tecnologia da Informação e Comunicação realizará a formatação do equipamento para garantir que nenhum programa ou dado seja acessível por terceiros nos casos em que a detenção, o uso, a posse ou a propriedade da máquina for transferida, sendo que tal medida restringir-se-á somente ao hardware.

13.1.8. Nenhum *software* poderá ser doado pela SPTrans a terceiros, salvo nos casos em que a licença assim o expressamente permitir.

13.1.9. A SPTrans poderá implantar e utilizar *softwares* e sistemas que possuam a funcionalidade de monitorar e gravar todas as atividades de uma estação ou equipamento de trabalho, assim como dados de navegação trafegados interna ou externamente para fins de gestão e auditoria.

13.1.10. Nos casos em que houver monitoramento remoto de uma estação de trabalho, o usuário deverá ser previamente comunicado por escrito pela Área competente.

13.1.11. A Área de Tecnologia da Informação e Comunicação poderá realizar inspeção em qualquer arquivo que estiver virtualmente armazenado na rede corporativa e em qualquer equipamento situado em local privado da Empresa estiver conectado na rede corporativa.

13.1.12. Os recursos de tecnologia e os ativos de informação da SPTrans deverão estar protegidos contra ataques de vírus, invasões e operações externas ou internas que eventualmente os exponham à perda de integridade ou outros riscos.

13.1.13. A informação classificada como restrita, sigilosa, secreta ou confidencial, deverá ser armazenada em diretórios de servidores que possuam *backup* automático sendo vedado o seu armazenamento em diretórios locais das estações de trabalho.

13.1.14. Não serão permitidas alterações na configuração física ou lógica dos recursos de tecnologia da Empresa, salvo nos casos de prévia justificativa e desde que autorizado pela Área de Tecnologia da Informação e Comunicação.

13.1.15. Todas as conexões da rede interna da SPTrans com redes externas deverão operar por meio de soluções seguras e monitoradas, com roteadores e *firewalls* e a geração de eventos de segurança, devendo estar sempre ativa e ser periodicamente analisada.

13.1.16. Todos os computadores portáteis e quaisquer equipamentos utilizados remotamente ou em teletrabalho que estiverem autorizados pela TIC a conectar a rede corporativa ou aos sistemas de informação da SPTrans deverão ser configurados com um *firewall* pessoal e antivírus.

13.1.17. O tempo de conexão dos usuários deverá ser restrito em áreas e em aplicações de alto risco de incidentes de segurança da informação.

13.1.18. Procedimentos formais deverão ser conduzidos para gerenciar o acesso à informação, como:

a. Registro de novos usuários;

b. Gerenciamento de senhas de usuários; e

c. Reavaliação ou revogação de acesso.

13.1.19. A identificação de usuário, sempre que possível, não poderá apresentar indicação dos direitos de acesso e nem o respectivo cargo ocupado na Empresa.

Nota: as exceções deverão ser solicitadas à Área de Tecnologia da Informação e Comunicação.

13.1.20. Todo computador deverá preferencialmente ter criptografia completa de disco rígido, quando possível, para impedir que usuários não autorizados acessem as informações nele armazenadas.

13.1.21. Toda mídia removível, tais como: pen drive USB, disco rígido portátil, CD e DVD gravável, deverá preferencialmente ser sistematicamente criptografada pelo usuário ou pela Área de Tecnologia da Informação e Comunicação, com o objetivo de impedir que usuário não autorizado acesse as informações armazenadas.

13.1.22. Toda mídia de *backup*, tais como, LTO e DLT, HD SATA e HD SSD também deverá ser criptografada para impedir que terceiro não autorizado acesse as informações armazenadas.

13.1.23. Qualquer *smartphone* corporativo que contiver dados restritos, sigilosos, secretos ou confidenciais da SPTrans deverá ser criptografado pela Área de Tecnologia da Informação e Comunicação.

13.1.24. O acesso a dados confidenciais deverá ser feito sempre por meio de um aplicativo, nunca diretamente pelo usuário.

13.1.25. Qualquer acesso a aplicação deverá ser precedido de autenticação e controle de acesso a recursos, de modo a permitir rastreamento das operações realizadas.

13.1.26. A estação e o terminal de trabalho deverão ser protegidos contra uso não autorizado, por meio de dispositivo de bloqueio, quando não estiverem em uso.

13.1.27. A proteção de tela deverá ser utilizada com senha, para garantir a segurança e a confidencialidade das informações.

13.1.28. Os usuários finais não deverão possuir nenhum direito ou privilégio de Administrador em seus computadores, estações ou terminais de trabalho.

13.1.29. Os procedimentos previstos nos itens anteriores deverão ser adotados para garantir o suporte eficiente às questões relacionadas aos usuários, a fim de manter os níveis de segurança definidos pela SPTrans na disponibilização dos computadores.

13.1.30. Para assegurar a oportuna resolução dos problemas e solicitações dos usuários finais é necessário o gerenciamento centralizado e automatizado das implantações de manutenção, correções e pacote de serviços.

13.1.31. O usuário deverá fazer manutenção periódica no diretório local do computador para evitar acúmulo de arquivos inúteis ou alheios às suas atividades, mantendo apenas arquivos temporários de trabalho.

13.1.32. Os arquivos permanentes de trabalho deverão ser mantidos pelo usuário em pastas compartilhadas na rede corporativa da SPTrans, as quais deverão contar com cópias periódicas de segurança.

13.2. Procedimentos de Operação dos Equipamentos

13.2.1. É proibida qualquer tentativa de obter acesso não autorizado, o que enseja em tentativa de fraudar autenticação ou segurança de qualquer servidor, rede ou conta.

13.2.2. É proibida qualquer tentativa de interferir nos serviços de qualquer servidor, rede ou outro usuário o que inclui, por exemplo, ataques do tipo "negativa de acesso", provocar congestionamento em redes, tentativas deliberadas de sobrecarregar um servidor e tentativas de invadir um servidor.

13.2.3. É proibido o uso de qualquer tipo de programa ou comando designado a interferir na sessão de usuários.

13.3. Diretório no Servidor de Arquivos

13.3.1. Toda Área da Empresa deverá ter espaço no servidor, em forma de diretório, com limite de armazenamento de dados previamente definido pela Área de Tecnologia da Informação e Comunicação.

13.3.2. O acesso ao diretório previsto no item **13.3.1** será apenas para os usuários pertencentes à mesma Área da Empresa.

Nota: caso haja a necessidade de se disponibilizar o acesso para usuários não pertencentes à mesma Área, deverá ser aberto um chamado técnico para a Área de Tecnologia da Informação e Comunicação, contendo a justificativa das Áreas envolvidas nesse procedimento.

13.3.3. Cada Área será responsável pelo gerenciamento de seu diretório no servidor de arquivos, devendo ser apagados arquivos duplicados e arquivos sem utilidade.

13.3.4. Caso seja necessário manter arquivos duplicados e arquivos sem utilidade por mais tempo no diretório, deverá ser aberto um chamado para a Área de Tecnologia da Informação e Comunicação, a qual é responsável por realizar o backup do Servidor de Arquivos.

Nota: após a confirmação da realização do backup, os arquivos duplicados e os arquivos sem utilidade deverão ser apagados.

13.3.5. Todos os arquivos importantes e relacionados às atividades institucionais da SPTrans deverão ser armazenados em pasta compartilhada do Servidor de Arquivos, não no diretório local da estação de trabalho.

13.3.6. O acesso e as aprovações às pastas de rede dar-se-ão de forma automática por meio do sistema de informação, nos quais os respectivos Gestores da informação já deverão estar previamente cadastrados.

13.3.7. É proibida a produção, edição, distribuição ou exposição e armazenamento, nos sistemas de informação da SPTrans, de qualquer material que viole qualquer lei ou regulamentação em vigor no território nacional, tais como:

a. Material de qualquer natureza que induza ou incite racismo, nazismo, discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional ou qualquer outro ato descrito pela legislação nacional como crime;

b. Material protegido por copyright;

c. Material cujo conteúdo esteja relacionado a sexo, drogas, pornografia, pedofilia, violência e armamento;

d. Marcas registradas;

e. Segredo comercial ou qualquer direito de propriedade intelectual usado sem a devida autorização.

f. Material difamatório, que constitua uma ameaça ilegal à SPTrans ou a terceiros.

13.3.8. É também proibida a produção, edição, distribuição ou exposição e armazenamento, nos sistemas de informação da SPTrans, de qualquer material obsceno e de quaisquer materiais ou arquivos não relacionados às atividades institucionais da SPTrans.

13.3.9. Os equipamentos e o servidor de arquivos da SPTrans não poderão ser utilizados para desenvolvimento, distribuição e gravação de programas, aplicativos, filmes, vídeos, arquivos de áudio, executáveis e jogos, exceto os que forem relacionados às atividades desenvolvidas pela Empresa e mediante prévia e expressa autorização da Área competente.

13.3.10. Não é permitido criar nem remover arquivos fora da área alocada ao usuário ou que venham a comprometer o desempenho e funcionamento dos sistemas de informação da SPTrans.

13.3.11. É proibido aos usuários realizar a instalação e a remoção de *softwares* dos equipamentos da Empresa.

Nota: havendo motivada necessidade para a instalação ou para a remoção de determinado *software*, a Área interessada deverá realizar a abertura de chamado técnico para a Área de Tecnologia da Informação e Comunicação.

13.3.12. É proibida ao usuário a abertura física de computadores ou de outro componente físico da rede para qualquer tipo de reparo, à exceção para troca de suprimentos (cartucho de tinta, papel etc).

Nota: caso seja necessária a realização de qualquer tipo de reparo no *hardware*, o interessado deverá efetuar a abertura de chamado para a Área de Tecnologia da Informação e Comunicação.

13.3.13. É proibida qualquer alteração de configurações de rede e de inicialização das máquinas bem como das estações de trabalho.

13.3.14. É proibido o acesso à rede lógica da SPTrans por um usuário utilizando o acesso fornecido por outro usuário.

13.3.15. É proibido a terceiros não autorizados o acesso aos sistemas de informação e às aplicações da SPTrans.

13.4. Acesso à Internet

13.4.1. Todo usuário é responsável pelo uso correto da Internet para minimizar os riscos aos recursos de TIC da SPTrans.

13.4.2. O acesso à Internet, na SPTrans será feito por meio das mesmas redes de comunicação que os sistemas se utilizam.

13.4.3. Todos os usuários deverão estar cientes da carga que provocam na rede em razão do acesso à Internet.

13.4.4. A Internet deverá ser utilizada para minimizar custos e maximizar o valor e a eficiência das atividades institucionais da SPTrans.

13.4.5. Os recursos de TIC da SPTrans não poderão ser utilizados pelos usuários para fazer *download*, cópia ou distribuição de software ou de dados ilícitos.

13.4.6. Os usuários não poderão fazer *download* de *softwares* ou aplicações da Internet (*freeware* ou *shareware*), sendo que exceções serão tratadas pela Área de Tecnologia da Informação e Comunicação.

13.4.7. É proibido copiar, revelar, transferir, examinar, renomear, trocar ou deletar informações ou programas pertencentes à SPTrans ou pertencentes ao proprietário ou titular da informação.

13.4.8. O uso da Internet deverá priorizar as atividades relacionadas aos serviços e atividades institucionais da SPTrans, à comunicação com parceiros, convenentes, terceirizados, credenciados e fornecedores, às pesquisas de tópicos pertinentes e à obtenção de informações empresariais úteis,

com a finalidade de manter os níveis mais altos de eficiência, qualidade e atualização técnica.

13.4.9. O uso da Internet para atividades pessoais deverá ser restrito para casos excepcionais.

13.4.10. Os usuários não poderão desenvolver qualquer atividade que ameace, interrompa ou comprometa a integridade e a segurança dos recursos de TIC da SPTrans, ou que, de outra maneira, resulte em seu uso impróprio, comprometendo o desempenho do ambiente de tecnologia da Empresa.

13.4.11. Todos os arquivos gerados pelos mecanismos que viabilizam os serviços de Internet poderão ser monitorados e armazenados pela SPTrans, para posterior análise e verificação do cumprimento desta Política pelas Áreas de competência.

13.4.12. Quando da percepção de qualquer ameaça ou falha de segurança ou do recebimento inadvertido de informações de origem desconhecida, a Área de Tecnologia da Informação e Comunicação ou o superior imediato deverá ser avisado imediatamente pelo usuário.

13.4.13. A Área de Tecnologia de Informação e Comunicação poderá gerar relatórios sobre o conteúdo e sobre a forma de utilização dos recursos de TIC acessados pelos usuários, relatórios estes que poderão ser alvo de auditoria das Áreas competente.

13.4.14. É proibida a utilização de aplicativos P2P ou *peer-to-peer* (ponto a ponto)

13.4.15. É proibida a utilização de serviços de entretenimento, tais como, sites de músicas, jogos, redes sociais, *streaming* de produções de vídeo e afins.

13.4.16. O uso de ferramenta de mensagem instantânea não corporativa não é permitido, sendo que exceções deverão ser aprovadas pela Área de Tecnologia de Informação e Comunicação e previamente justificadas pela Área interessada.

13.5. Utilização de E-mail

13.5.1. O correio eletrônico da SPTrans deverá ser utilizado apenas para fins institucionais, de forma individual e discriminada, por intermédio exclusivo do *software* disponibilizado pela Área de Tecnologia da Informação e Comunicação.

13.5.2. Nos casos de ameaça ou de risco à SPTrans, a Área de Tecnologia da Informação e Comunicação, após consulta à Área Jurídica e mediante prévia e expressa autorização da Diretoria da Área envolvida na ocorrência, poderá acessar o conteúdo da conta de e-mail corporativo de qualquer usuário da Empresa.

13.5.3. Não deverá ser enviada à rede externa informação classificada como restrita, secreta, sigilosa ou confidencial.

13.5.4. É proibido ao usuário emitir opinião por e-mail em nome da SPTrans, a não ser que esteja formalmente autorizado pela Diretoria da Área.

13.5.5. Todo usuário deverá ter sua própria conta de e-mail, não devendo compartilhá-la com ninguém em nenhuma hipótese.

13.5.6. O e-mail não poderá conter mensagens abusivas, obscenas, racistas, discriminatórias, constrangedoras ou difamatórias, nem comentários que possam causar danos à SPTrans ou a terceiros.

13.5.7. É proibido o envio de *spam* e de mensagens que contenham vírus ou ameaças à segurança da SPTrans ou de terceiros, assim como reenviar ou de qualquer forma propagar mensagem em cadeia, corrente ou "pirâmide".

13.5.8. Estagiário, menor aprendiz ou prestador de serviço somente deverá ter conta de e-mail se estritamente necessário à execução de suas atividades e formalmente justificado e autorizado pela Área envolvida.

13.5.9. Prestadores de serviço não poderão enviar mensagens externas aos ambientes da SPTrans.

13.5.10. Toda mensagem criada e armazenada nos computadores ou redes da SPTrans é de propriedade corporativa e não deverá ser tratada como pessoal.

13.5.11. Quando da percepção de qualquer ameaça ou falha de segurança ou do recebimento inadvertido de informações de origem desconhecida, a Área de Tecnologia da Informação e Comunicação ou o superior imediato deverá ser avisado imediatamente pelo usuário.

13.5.12. Arquivos e links encaminhados por e-mail de origem desconhecida não deverão ser abertos pelos usuários da SPTrans.

13.5.13. Os usuários não poderão enviar mensagens de e-mail cuja quantidade prejudique ou tenha o potencial de prejudicar a eficiência ou a capacidade da rede, tais como mala direta com, por exemplo, publicidade, anúncios e informativos alheios às atividades institucionais da SPTrans.

13.5.14. Será bloqueado pela SPTrans qualquer e-mail com arquivo anexo de tamanho excessivo, que comprometa ou que tenha potencial de comprometer o uso de banda ou prejudique o funcionamento dos sistemas e serviços regulares, sendo que, em casos de justificada necessidade, deverá ser solicitada autorização à Área de Tecnologia da Informação e Comunicação para agendamento, evitando comprometer a performance da rede.

13.5.15. É obrigatória a realização pelos usuários de limpeza periódica da caixa de e-mail, evitando acúmulo de arquivos inúteis, seguindo os limites estabelecidos para o tamanho das caixas postais. Quando do recebimento das mensagens automáticas de alerta sobre esses limites, caberá ao usuário executar a limpeza de mensagens armazenadas no servidor de correio eletrônico.

13.5.16. É obrigatória a utilização de assinatura padronizada no e-mail no formato publicado na Intranet através da rotina “Gerador de Assinatura”.

Nota: é proibido constar o número de telefone particular do usuário nas mensagens encaminhadas através da conta de e-mail corporativo.

14. ADMINISTRAÇÃO DE SERVIDORES

14.1. O gerenciamento de servidores da SPTrans deverá incluir:

a. Ativação e desativação de equipamentos;

b. Instalação e configuração;

c. *Backup* de dados;

d. Manutenção de equipamentos;

e. *Service Level Agreement* – SLA;

f. Plano de Contingência;

g. Configuração e administração do ambiente de tecnologia;

h. Controle de acesso ao *Data Center*, sala de comunicação, sala de UPS (fonte de alimentação ininterrupta) e ativos de rede; e

i. Reinicialização e recuperação.

14.2. O Plano de Contingência de que trata o item **14.1**, subitem f, deverá estabelecer procedimentos que assegurem a operação e a recuperação de ativos de informação em situações de emergência, de acordo com as necessidades e prazos específicos.

14.3. As atividades e o estado da rede deverão ser constantemente monitorados pela Área de Tecnologia da Informação e Comunicação para prevenção de incidentes e para planejamento da capacidade dos equipamentos.

15. VIRTUAL PRIVATE NETWORK – VPN

15.1. O usuário da SPTrans deverá utilizar a *Virtual Private Network* – VPN para ter acesso remoto aos computadores e à rede corporativa da SPTrans.

15.2. Caso o usuário não tenha equipamento da SPTrans, e em caso de necessidade comprovada e autorizada, a Área de Tecnologia da Informação e Comunicação providenciará o empréstimo de equipamento.

15.3. A solicitação de acesso à VPN deverá ser apresentada à Área de Tecnologia de Informação e Comunicação pela Área interessada com antecedência mínima de 3 (três) dias.

15.4. O acesso à VPN, na hipótese prevista no item 15.2, será temporário e definido por escrito pela Área de Tecnologia da Informação e Comunicação.

15.5. O acesso permanente à VPN será permitido como padrão ao perfil dos usuários que:

a. fizerem uso do acesso remoto como parte de suas atividades funcionais;
b. exercerem atividades em regime integral ou parcial de teletrabalho;
c. utilizarem notebook cedido pela SPTrans;
d. exercerem atividades externas;
e. ocuparem o cargo de Presidente, Diretor, Superintendente, Gerente, Auditor, Analista de Sistemas e Desenvolvedor, Analista de Produção e Infraestrutura de TI, exceto HelpDesk, desde que exerçam atividades externas e desde que haja necessidade de acesso remoto.

16. ANÁLISE DE LOGS DE ACESSO

16.1. A Área de Segurança de Informações enviará relatório com os *logs* de acessos dos usuários nos ambientes operacionais para a Área de Tecnologia da Informação e Comunicação para análise de auditoria nas bases de dados, e, em caso de suspeita de uso indevido, reportará esses casos à Diretoria a que estiver subordinada.

16.2. A Área de Tecnologia da Informação e Comunicação deverá comunicar toda e qualquer utilização indevida de acessos e senhas à Diretoria a que estiver subordinada e ao responsável da Área a que se reportar o usuário que estiver envolvido no incidente.

16.3. Os acessos indevidos aos sistemas de informação da SPTrans deverão ser imediatamente bloqueados.

Nota: em casos de reincidência, a Área de Auditoria Interna deverá ser informada.

17. DESENVOLVIMENTO DE SEGURANÇA DE SISTEMAS

17.1. As atividades de desenvolvimento de sistemas, de testes e de migração de programas e sistemas entre ambientes deverão ser conduzidas de maneira controlada e segura, seguindo as melhores práticas de mercado.

17.2. Os programas fontes os programas compilados que estiverem em fase de desenvolvimento ou em manutenção deverão ser mantidos em bibliotecas do ambiente de desenvolvimento.

17.3. Controles de segurança deverão ser planejados e definidos na fase de análise de requerimentos do desenvolvimento de um sistema, de forma a fazer parte do sistema desde o início de sua implementação.

17.4. Todo projeto de desenvolvimento de sistema deverá contemplar os seguintes aspectos, sem limitar-se a eles:

a. Entrevistas, levantamento de requisitos e definição de escopo;

b. Acompanhamento das prioridades nas etapas estabelecidas do projeto;

c. Relatórios de administração do projeto com objetivo e status;

d. Utilização de *software* auxiliar no acompanhamento do progresso do projeto;

e. Testes e homologação.

17.5. A documentação dos sistemas deverá conter informações específicas sobre os controles de segurança, de maneira que os usuários fiquem cientes de sua existência.

17.6. O acesso a sistemas, aplicações e bases de dados necessários à condução de um trabalho deverá ser restrito a responsáveis, analistas e desenvolvedores.

17.7. A definição dos controles de segurança deverá considerar as seguintes necessidades:

a. Controlar o acesso aos ativos da informação, inclusive requisitos de segregação de tarefas e ambientes;

b. Produzir trilhas de auditoria;

c. Verificar e proteger a integridade de dados críticos;

d. Proteger a informação contra acesso não autorizado;

e. Utilizar criptografia para proteger dados críticos de negócio, quando transmitidos ou armazenados, se possível;

f. Proteger a informação contra modificação não autorizada;

g. Estar em conformidade com requisitos legais, fiscais e contratuais;

h. Realizar, no mínimo, uma cópia *backup* dos dados críticos do negócio;

i. Recuperar falhas, especialmente em sistemas com requisitos de alta disponibilidade;

j. Habilitar o sistema a ser operado e usado de forma segura por pessoal não especializado, porém treinado; e

k. Para toda aplicação desenvolvida, validar a entrada de dados, com o intuito de garantir a integridade dos dados manipulados pela aplicação.

17.8. Para todo sistema desenvolvido, deverão ser incorporados mecanismos de proteção contra falhas de processamento e contra atos intencionais que possam alterar indevidamente os dados manipulados pelo sistema.

17.9. Para todo sistema desenvolvido que envolva transmissão de mensagens, deverá ser feita análise dos riscos de segurança, para determinar se é legítimo ou não o emprego da técnica de autenticação de mensagens e, em caso afirmativo, qual o melhor método de implementação da técnica.

17.10. Deverá ser evitado o uso de dados reais no processo de teste dos sistemas.

17.11. Nenhum processo de desenvolvimento de sistemas deverá alterar informações dos ambientes de produção.

17.12. Todo sistema desenvolvido deverá passar por um processo completo de testes e de controle de mudanças, antes de ser liberado à produção.

17.13. O código-fonte de programa deverá ser devidamente controlado e armazenado em local seguro.

17.14. Todo ambiente de desenvolvimento e manutenção deverá ser estritamente controlado, de modo a garantir que as mudanças sejam revistas, segregadas e aprovadas, antes de realizadas no ambiente de produção.

17.15. A passagem de um novo programa ou sistema, ou alterações em programa ou sistema existente, do ambiente de testes para o de produção deverá ser rigorosamente controlada, explicitamente autorizada pelos profissionais envolvidos e devidamente documentada.

18. DISPOSITIVOS REMOVÍVEIS

18.1. O acesso a dispositivo de armazenamento removível para usuário somente poderá ser realizado conforme procedimentos abaixo:

18.1.1. O usuário interessado deverá previamente justificar por escrito a necessidade de utilização do dispositivo de armazenamento removível e declarar que:

a. assume toda e qualquer responsabilidade pelo acesso e pelo tratamento das informações armazenadas no dispositivo;
b. recebeu todas as instruções para o correto uso do dispositivo de armazenamento removível;
c. está ciente da confidencialidade das informações eventualmente contidas no dispositivo de armazenamento removível e que elas deverão somente ser utilizadas em atividades institucionais da SPTrans;
d. está ciente da presente Política e das demais normas internas que tratarem de Segurança da Informação.

18.1.2. O Diretor e o Superintendente da Área do usuário solicitante deverão autorizar por escrito o acesso do usuário ao dispositivo de armazenamento removível.

18.1.3. O acesso ao uso de dispositivos de armazenamento removível será permitido como padrão ao perfil dos usuários que:

a. utilizam o dispositivo de armazenamento removível como parte de seu trabalho devido ao uso de equipamentos cedidos pela SPTrans, tais como, máquina fotográfica, *notebook* e telefone móvel;
b. ocuparem o cargo Presidente, Diretor, Superintendente e Gerente, exercendo ou não atividades externas, desde que haja comprovada necessidade.

19. ADMINISTRAÇÃO DE LICENÇAS DE SOFTWARES

19.1. Todo *software* instalado deverá possuir licença válida de uso.

19.2. A Área de Tecnologia da Informação e Comunicação é responsável por manter e por controlar as licenças dos *softwares* instalados, realizando o gerenciamento dessas licenças de software adquiridas e utilizadas pela SPTrans em conformidade com a legislação vigente e com a presente Política.

19.3. Nenhum *software* deverá ser copiado, exceto nos casos especificados nos termos de licenciamento e previamente autorizados pela Área de Tecnologia da Informação e Comunicação.

19.4. Toda instalação de *software* deverá ser realizada ou reconhecida pela Área de Tecnologia da Informação e Comunicação.

19.5. Nenhum *software*, mesmo *freeware*, deverá ser instalado no ambiente de rede da SPTrans.

19.6. A distribuição e o controle dos *softwares* na SPTrans serão feitos por meio de ferramenta que permita a emissão de inventário.

19.7. O inventário dos *softwares* deverá ser mantido sempre atualizado pela Área de Tecnologia da Informação, o que concorrerá para a proteção efetiva, tornando-se a base para a realização da classificação da informação e para a atribuição da propriedade desses ativos.

19.8. O suporte de *softwares* e de *hardwares* deverá ser prestado pelos próprios fornecedores.

20. VÍRUS E SOFTWARES MALICIOSOS

20.1. O software de antivírus deverá examinar todos os arquivos, em busca de vírus conhecidos, tão logo servidores, estações de trabalho e equipamentos sejam ligados, permanecendo ativo durante todo o período em que o equipamento estiver ligado.

20.2. Todo arquivo ou software recebido de terceiros deverá ser previamente examinado pela Área de Tecnologia da Informação e Comunicação antes de sua instalação no ambiente de produção.

20.3. Todo arquivo ou mídia recebido de fonte externa deverá passar por uma varredura antivírus, antes de ser utilizado e antes de ser enviado a outro destinatário.

20.4. Somente mídia e *software* licenciado e homologado poderão ser instalados na rede da SPTrans pela Área de Tecnologia da Informação e Comunicação.

20.5. O *boot* pelos drives externos é restrito à Área de Tecnologia da Informação e Comunicação.

20.6. É proibido abrir arquivo executável recebido via e-mail.

Nota: a Área de Tecnologia de Informação e Comunicação deverá ser imediatamente comunicada pelo usuário através da abertura de chamado via HelpDesk.

20.7. O controle de acesso interno e externo à rede SPTrans é assegurado por meio de *firewall* e qualquer incidente deverá ser prontamente comunicado à Área de Tecnologia da Informação e Comunicação.

20.8. O *backup* dos dados mantidos em servidores será realizado regularmente.

21. VIOLAÇÕES E PENALIDADES

21.1. 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.

22. DISPOSIÇÕES FINAIS

22.1. Esta Política será sucedida por outros instrumentos normativos complementares específicos, os quais deverão manter a coesão com as regras, diretrizes e princípios aqui estabelecidos.

22.2. A SPTrans deverá implementar as instruções contidas nesta Política, bem como editar os instrumentos de que trata o item 21.

22.3. A presente Política e as demais normas e procedimentos de segurança da informação deverão ser divulgadas nos canais de transparência pública e estar disponíveis para consulta nos canais internos da Empresa.

22.4. Em caso de suspeita, ameaça ou ocorrência de incidente de segurança, a Área de Tecnologia da Informação e Comunicação deverá ser comunicada formal e imediatamente.

22.5. Em caso de dúvidas quanto a esta Política ou aos demais procedimentos de segurança da informação, o usuário deverá solicitar os esclarecimentos necessários para a Área de Tecnologia da Informação e Comunicação.

22.6. A presente Política deverá ser revista e atualizada em intervalo não superior a três anos ou sempre que se julgar necessário.

23. APROVAÇÕES

Esta Política de Segurança da Informação foi aprovada pela Diretoria Executiva em 19 de outubro de 2021 e pelo Conselho da Administração em 26 de outubro de 2021.

24. REVISÕES

HISTÓRICO DE REVISÕES		
REVISÃO	DATA	ALTERAÇÃO
0	29.10.21	Emissão inicial.