VERSÃO 1.01

13/12/2022

PARQUE TECNOLÓGICO
São José dos Campos

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

ASSOCIAÇÃO PARQUE TECNOLÓGICO DE SÃO JOSÉ DOS CAMPOS

DOCUMENTO ATUALIZADO EM 03/03/2022

Controle de Versão			
Tratamento	**Versão**	**Autor**	**Emissão**
Criação	1.0	Peduti Advogados	23/02/2022
Revisão	1.01	Baikal Security	03/03/2022

1. INTRODUÇÃO

1.1. Esta Política de Segurança da Informação ("Política") estabelece as medidas a serem tomadas por todos os funcionários do **APTSJC,** a fim de proteger os dados e as informações (em formato eletrônico ou não) tratados em todas as suas fases (criação, manuseio, armazenamento, transporte ou descarte) e para proteger os sistemas de computadores, dispositivos, infraestrutura, ambiente de computação (coletivamente, "Sistemas de TI") do **APTSJC** e todo e qualquer outro ativo de informação de danos, ameaças internas, externas, deliberadas ou acidentais.

2. OBJETIVO

2.1. O principal objetivo desta Política é estabelecer as diretrizes e responsabilidades para assegurar a confidencialidade, integridade e disponibilidade dos dados, informações, documentos e conhecimentos produzidos, armazenados ou transmitidos, bem como proteger a organização contra ameaças e vulnerabilidades de modo a preservar os seus ativos de informação, sua reputação e imagem institucional, segundo os requisitos do negócio e as leis e regulamentações vigentes.

2.2. Para os fins desta Política:

2.2.1. "Titular": têm o significado definido no Artigo 5º, inciso V da lei 13709/18, a qual se refere a pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

2.2.2. "Dados pessoais" têm o significado definido no Artigo 5º, inciso I da lei 13709/18, Lei Geral de Proteção de Dados ("LGPD"): qualquer informação relativa a uma pessoa física identificada ou identificável (um "titular dos dados"); uma pessoa física identificável é aquela que pode ser identificada, direta ou indiretamente, em particular por referência a um identificador, como um nome, um número de identificação, dados de localização.

2.2.3. " Dados sensíveis" têm o significado definido no Artigo 5º, inciso II da lei 13709/18, Lei Geral de Proteção de Dados ("LGPD"): qualquer

informação 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 vinculado a uma pessoa natural;

3. DEFINIÇÕES

Ameaça: conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou para a organização.

Antivírus: software especializado em prevenir, detectar, remover e restaurar as informações e sistemas de possíveis ataques de vírus.

Ativo ou Ativos Informacionais: conjunto de informações que são recepcionadas com valor real ou potencial para a organização, podendo ser físico ou não, como bases de dados e arquivos: documentação de sistema, informações sobre pesquisas, manuais de usuários, materiais de treinamento, procedimentos de suporte ou operação, planos de continuidade do negócio, procedimentos de recuperação, trilhas de auditoria e informações armazenadas.

Confidencialidade: garantia de que a informação seja acessada a quem se destina, respeitando a classificação: confidencial (o mais alto nível de confidencialidade), restrita (médio nível de confidencialidade), uso interno (o mais baixo nível de confidencialidade) e pública (todos podem ver a informação).

Criptografia: técnica utilizada para codificar informações e permitir que somente pessoas autorizadas consigam acessá-las.

Disponibilidade: garantia de que a informação esteja disponível sempre que se necessite dela.

Encarregado de Proteção de Dados - Data Protection Officer (DPO): pessoa física ou jurídica responsável que tem responsabilidade pela proteção de dados dentro de uma organização, garantindo a segurança das informações de clientes, fornecedores e da própria empresa.

Incidente de segurança da informação: evento que causa ou possa causar a interrupção, a redução e/ou afetar à confidencialidade, integridade e disponibilidade dos sistemas, serviços e ativos de TI da organização.

Integridade: garantia de que a informação não seja modificada ou danificada, acidentalmente ou intencionalmente.

Informação: dados, processados ou não, que possam ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato.

Malware: qualquer tipo de software (programa) que possua código malicioso, popularmente conhecido como Vírus. São classificados principalmente em *Ransomwares, Worms*, Cavalos de Tróia, *Spywares*, *Malwares*, *Adwares*, dentre outros, conforme o tipo de dano ou objetivo causado ao sistema.

Operador de dados: pessoa física ou jurídica responsável pelo tratamento de dados.

Sistemas de Informação: sistema automatizado que contempla pessoas, máquinas, e/ou métodos organizados para coletar, processar, transmitir e disseminar dados que representam informação para o usuário.

Usuários: funcionário, estagiário ou terceiro com cadastro (usuário) na rede de computadores da organização, para acessar os sistemas de informação e recursos de computação do **APTSJC**

Vulnerabilidade: fraqueza de um ativo de informação que possa ser potencialmente explorada por uma ou mais ameaças.

Violação de dados pessoais: qualquer evento relacionado à violação da segurança com dados pessoais de forma acidental ou intencional, e que resulte na destruição, perda, alteração, vazamento ou ainda, qualquer forma de tratamento de dados inadequada ou ilícita, os quais possam ocasionar risco para os direitos e liberdades do titular dos dados pessoais.

4. APLICAÇÃO

4.1. Esta Política aplica-se a todos os colaboradores da **APTSJC,** parceiros de negócios e fornecedores que tratem as informações da organização para qualquer fim. A presente Política passa a vigorar a partir da data de sua aprovação e publicação, sendo válida por tempo indeterminado.

4.2. Todos os colaboradores da **APTSJC** e quaisquer terceiros habilitados a usar os Sistemas de TI e os dados coletados, mantidos e tratados pela **APTSJC**, englobando, mas não se limitando a, contratados e subcontratados

(coletivamente, "Usuários"), são responsáveis pelo cumprimento da presente Política, bem como devem garantir a sua aplicação e entendimento com treinamentos regulares.

5. PRINCÍPIOS

5.1. Todos os dados pessoais e sensíveis tratados pela **APTSJC** serão utilizados exclusivamente em conformidade com o teor desta Política e da LGPD, quando aplicável.

5.2. Todos os Sistemas de TI deverão ser instalados, mantidos, reparados e atualizados pelo Responsável de Tecnologia e Segurança da Informação do **APTSJC** ou por empresa autorizada a prestar esse tipo de serviço.

5.3. Todos os sistemas e dados serão protegidos a todo custo contra acessos não autorizados.

5.4. Todos os dados, não se limitando aos de classificação pessoal, deverão ser tratados com segurança, observando não só a LGPD, mas toda legislação e normativas que versem sobre a privacidade e proteção de dados, vigentes nesta data ou em momento superveniente.

5.5. Todos os Sistemas de TI, dados e informações deverão ser usados apenas em conformidade com as políticas e procedimentos da **APTSJC.**

5.6. Todos os dados deverão ser classificados de forma adequada (incluindo, mas não se limitando a, dados pessoais, dados pessoais sensíveis e informações confidenciais).

5.7. Todos os dados, sejam por meio físico ou digital, estarão disponíveis apenas para os Usuários com necessidades legítimas de acesso e deverão ser protegidos contra acesso e/ou processamento não autorizado ou inadequado.

5.8. A responsabilidade pela segurança dos dados e informações, sejam no âmbito tecnológico ou não, é um dever de todos da **APTSJC**. A função de manter a segurança de todos os Sistemas de TI e dos dados neles armazenados (incluindo, mas não se limitando a, segurança, integridade e confidencialidade desses dados) é do Operador de Dados.

5.9. Cabe ao Encarregado de Proteção de Dados (DPO) manter o monitoramento para que seja garantida segurança e a conformidade da proteção da

privacidade dos dados pessoais da organização, em observância às políticas internas e à LGPD.

Nome: Caroline Cubas Lopes – Assessora Jurídica

E-mail: lgpd@pqtec.org.br

5.10. Todas as violações de segurança dos Sistemas de TI ou de quaisquer dados neles armazenados serão identificados, relatados e devidamente investigados pelo Responsável pela Segurança da Informação. Qualquer violação que seja conhecida ou suspeita de envolver dados pessoais deverá ser relatada ao Operador de Dados e ao DPO, Eduardo Basílio e Caroline Cubas Lopes, respectivamente.

5.11. Todos os Usuários deverão obrigatoriamente relatar todas e quaisquer preocupações de segurança da informação relacionadas aos Sistemas de TI ou aos dados armazenados neles, imediatamente para o Coordenador de TI do **APTSJC**. Caso alguma dessas preocupações se relacionem de alguma forma com dados pessoais, também deverão ser relatadas ao DPO e Operador de Dados.

6. RESPONSABILIDADES DOS DEPARTAMENTOS

6.1. O Operador de Dados, conforme o artigo 39 da Lei Geral de Proteção de Dados, e o Departamento de Tecnologia da Informação serão responsáveis por:

a) Contribuir com o bom entendimento dos Usuários para o cumprimento dos aspectos relacionados à TI e apoio nas questões relacionadas à Segurança da Informação desta Política;

b) Fornecer a todos os Usuários suporte e treinamento adequados em questões de segurança de TI e uso de Sistemas de TI;

c) Garantir que os Usuários possuam os níveis de acesso aos sistemas e ativos de TI convenientes e limitados, levando em consideração a sua função, cargo e responsabilidade na escala organizacional;

d) Receber e tratar todos os relatórios relativos a questões de segurança de TI e tomar as medidas adequadas em resposta;

e) Tomar medidas proativas, para garantir que o Usuário entenda os procedimentos relativos à segurança da informação e implementar medidas de segurança adequadas à proteção e segurança da informação;

f) Tomar todas as medidas necessárias para implementar esta Política e quaisquer alterações feitas a esta Política no futuro; e

g) Garantir que a "Política de Backups" estabelecida para dados e informações armazenadas nos ativos de tecnologia, sejam realizados com a frequência e demais parâmetros previstos na política, garantindo que os backups sejam alocados, armazenados e transportados de forma segura, em observância aos melhores padrões de segurança do mercado.

6.2. O Encarregado de Proteção de Dados (DPO), será responsável por, em conformidade com o artigo 41, § 2º e incisos, da Lei Geral de Proteção de Dados:

a) Auxiliar todos os Usuários a compreender e cumprir os aspectos não relacionados à tecnologia da informação presentes nesta Política;

b) Fornecer a todos os Usuários suporte e treinamento adequados em questões de proteção de dados;

c) Garantir que todos os Usuários tenham níveis de acesso aos dados apropriados para cada Usuário, levando em consideração a sua função, cargo, responsabilidades e quaisquer requisitos especiais de segurança;

d) Receber e tratar relatórios relativos a questões de proteção de dados pessoais, tomar as medidas e promover as orientações adequadas para resposta;

e) Tomar medidas proativas, quando possível, para estabelecer e implementar procedimentos de proteção e aumentar a conscientização do Usuário; e

f) Auxiliar o Operador de Dados e o Departamento de TI no monitoramento da proteção de dados do **APTSJC** e tomar todas as medidas necessárias para implementar esta Política e quaisquer alterações feitas a ela no futuro.

7. RESPONSABILIDADE DE TODOS OS USUÁRIOS

7.1. Os Usuários devem obedecer e cumprir com os termos desta Política.

7.2. Todos os Usuários devem usar os Sistemas de TI e dados apenas dentro dos limites da legislação brasileira e não devem usar os Sistemas de TI ou dados para qualquer propósito ou atividade relativas que não estejam relacionadas ao escopo de seu contrato de trabalho,das políticas de integridades da **APTSJC,** que possa infringir qualquer normativa brasileira ou de qualquer outra parte do mundo, vigentes ou em vigor no futuro.

7.3. Os Usuários deverão informar ao Departamento de Tecnologia da Informação com cópia ao DPO, toda e qualquer preocupação relacionada a proteção de dados pessoais e a integridade da segurança digital do **APTSJC** e só poderão tomar ações após validação do **DPO.**

7.4. Os Usuários devem informar imediatamente à Equipe de TI sobre quaisquer outros problemas técnicos (incluindo, mas não se limitando a, falhas de hardware e erros de software) que possam ocorrer nos Sistemas de TI e ativos de tecnologia.

7.5. Toda e qualquer violação deliberada ou negligente desta Política pelos Usuários será considerada como falta grave, acarretando a aplicação das sanções, inclusive, falta grave previstas nos procedimentos internos da organização, bem como toda e qualquer legislação vigente no território brasileiro.

8. MEDIDAS DE SEGURANÇA DE SOFTWARES

8.1. Todos os softwares, incluindo, mas não se limitando a, sistemas operacionais, aplicativos, softwares individuais e *firmwares*, serão mantidos atualizados tão logo possível, após o lançamento de atualização, conforme procedimento estabelecido pelo Departamento de Tecnologia da Informação para gerenciamento de atualizações, ficando à critério da tecnologia da informação gerir e deliberar sobre o assunto.

8.2. Quando qualquer falha de segurança for identificada em qualquer software, o Operador de Dados e o Departamento de TI serão informados imediatamente, e essa falha será corrigida mediante procedimento adequado de correção, e caso possível, de modo imediato, ou o software poderá ser retirado dos ativos de tecnologia até que a falha de segurança possa ser corrigida de forma eficaz.

Caso haja suspeita de possível falha de segurança e de provável afetação de quaisquer dados pessoais, o DPO deverá ser informado imediatamente.

8.3. Nenhum Usuário poderá instalar ou executar qualquer tipo software, seja esse software fornecido em mídia física, ou seja, ele baixado, sem a aprovação do Coordenador de TI ou pessoa por ele designada. Qualquer software ainda não homologado pelo Departamento de Tecnologia da Informação, deverá ser aprovado mediante solicitação formal, e só poderá ser instalado ou executado após autorização, onde essa instalação não represente nenhum risco de segurança para os Sistemas de TI, bem como não viole nenhum contrato de licença a que esse software possa estar sujeito.

8.4. Todo software será instalado e configurado nos Sistemas de Tecnologia da Informação pelo Departamento de Tecnologia da Informação. Qualquer instalação ou execução de softwares não homologados e não autorizados pelo departamento, implicará em violação e será considerado como falta grave.

9. MEDIDAS DE SEGURANÇA ANTIVÍRUS

9.1. Todos os sistemas e ativos de tecnologia (incluindo todos os computadores e servidores) serão protegidos com antivírus, firewall e outros softwares de segurança adequados. Todos esses softwares serão mantidos atualizados com as medidas de segurança necessárias, bem como com as últimas atualizações disponíveis.

9.2. Todos os Sistemas de TI protegidos por software antivírus estarão sujeitos a uma verificação completa do sistema mensalmente ou em período inferior, se necessário.

9.3. As mídias físicas removíveis, como *pendrives* ou discos ou qualquer outro dispositivo semelhante, usadas para transferir dados e informações, por padrão serão bloqueadas nas máquinas. As exceções deverão ser habilitadas e autorizadas através justificativa e mediante autorização formal emitida pelo Departamento de Tecnologia da Informação do **APTSJC**, ocasião na qual os dispositivos de mídia deverão ser primeiramente verificados a sua seguridade.

9.4. Os Usuários devem ter permissão para transferir arquivos usando sistemas de armazenamento em nuvem apenas com a aprovação do Operador de Dados e do Departamento de TI

9.5. Todos os arquivos baixados de qualquer sistema de armazenamento em nuvem devem ser verificados em busca de vírus durante o processo de download.

9.6. Todos os arquivos enviados à terceiros fora dos domínios do **APTSJC**, utilizando qualquer meio de transferência física ou digital, deverão ser verificados em busca de risco relacionado à segurança da informação, nos termos do artigo 154-A do Código Penal[1] e da Lei nº 12.965/2014, Marco Civil da Internet. [2]

9.7. Sempre que qualquer vírus for detectado por um Usuário, o evento deverá ser relatado imediatamente ao Operador de Dados e o Departamento de Tecnologia da Informação esta regra se aplica mesmo quando o software antivírus corrige o problema automaticamente. O Operador de Dados e o Departamento de Tecnologia da Informação tomarão prontamente toda e qualquer ação necessária para solucionar o problema. Em circunstâncias limitadas, as medidas poderão envolver a remoção temporária do computador ou dispositivo afetado. Sempre que possível, um computador ou dispositivo de substituição adequado será fornecido para limitar a interrupção de atividades para o Usuário.

9.8. Se qualquer vírus ou outro malware afetar, tiver probabilidade de afetar ou houver suspeita de afetar quaisquer dados pessoais, além das medidas previstas nos itens acima, o problema deve ser relatado imediatamente ao DPO da **APTSJC.**

9.9. Quando qualquer Usuário introduzir deliberadamente qualquer software ou arquivo malicioso para os Sistemas de TI, incorrerá em ofensa criminal, nos termos do artigo 154-A do Código Penal e da Lei nº 12.965/2014, Marco Civil

---

[1] Art. 154-A. Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita

[2] https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm

da Internet, e será tratado conforme apropriado de acordo com os procedimentos legais e disciplinares do **APTSJC.**[3]

10. MEDIDAS DE SEGURANÇA DE HARDWARES

10.1. Sempre que possível, os Sistemas de TI estarão localizados em ambientes com acesso restrito ou concedido aos Usuários autorizados por meio de uma chave, *smart card,* código da porta ou similar de uso pessoal. Onde o acesso a tais locais for restrito, os Usuários não deverão permitir qualquer tipo de acesso por terceiros ou colaboradores não autorizados a tais locais, por qualquer motivo que seja.

10.2. Todos os Sistemas de TI não destinados ao uso normal pelos Usuários, incluindo, mas não se limitando a, servidores, equipamentos de rede e infraestrutura de rede, os quais deverão estar localizados, sempre que possível, em salas protegidas e climatizadas e/ou em gabinetes trancados que poderão ser acessados apenas por membros designados pelo Departamento de Tecnologia da Informação.

10.3. Nenhum Usuário deve ter acesso a quaisquer Sistemas de TI não destinados ao uso normal dos Usuários, incluindo os dispositivos mencionados acima no item 10.2, sem a permissão expressa do Coordenador de TI. Em circunstâncias normais, sempre que um problema com tais Sistemas de TI for identificado por um Usuário, esse problema deverá ser relatado ao Departamento de Tecnologia da Informação. Sob nenhuma circunstância um Usuário deve tentar retificar tais problemas sem a permissão expressa, instrução e/ou supervisão do Coordenador de TI.

10.4. Todos os dispositivos móveis não portáteis, incluindo, mas não se limitando a, computadores desktops, estações de trabalho e monitores, deverão, sempre que possível, serem fisicamente fixados no local com um mecanismo de travamento adequado. Onde o projeto do hardware permitir, os gabinetes de

[3] https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm

computadores deverão ser trancados para evitar adulteração ou roubo de componentes internos.

10.5. Todos os dispositivos móveis portáteis (incluindo, mas não se limitando a, laptops, tablets e smartphones) fornecidos pelo **APTSJC** deverão ser sempre transportados com segurança e manuseados com cuidado. Em circunstâncias excepcionais em que tais dispositivos móveis necessitem serem deixados sem supervisão, eles deverão ser colocados dentro de uma caixa com chave ou outro recipiente adequado com tranca. Os Usuários deverão como regra tomar todos os esforços razoáveis para evitar que tais dispositivos móveis sejam deixados sem supervisão em qualquer local, ainda que os equipamentos estejam em suas residências particulares ou nas instalações do **APTSJC**. Os dispositivos não deverão ser deixados em veículos sem supervisão. Contudo, em caso de excepcional necessidade de algum desses dispositivos móveis serem deixados em um veículo, deverão ser guardados fora da vista e, quando possível, em um compartimento trancado.

10.6. Em caso de furto, roubo ou extravio de qualquer dispositivo móvel portátil, deverá ser informado imediatamente ao Coordenador de TI para que sejam tomadas as medidas necessárias.

10.7. O Departamento de Tecnologia da Informação da **APTSJC** deverá manter um registro completo de ativos de todos os Sistemas de TI. Todos os Sistemas de TI deverão ser rotulados e os dados correspondentes deverão ser mantidos no registro de ativos.

11. SEGURANÇA ORGANIZACIONAL

11.1. Todos os Usuários que lidam ou realizam o tratamento de dados, em particular dados pessoais, deverão ser devidamente treinados para fazê-lo.

11.2. Todos os Usuários que lidam ou realizam o tratamento de dados, em particular dados pessoais, serão supervisionados de forma adequada por seus respectivos superiores profissionais.

11.3. Todos os Usuários que lidam ou realizam o tratamento de dados, em particular dados pessoais, deverão ser solicitados e incentivados a ter cuidado, cautela e

discrição ao discutir questões relacionadas ao trabalho relacionadas a tais dados pessoais, seja no local de trabalho ou de outra forma, em observância às políticas se segurança da informação e gestão de dados da **APTSJC.**

11.4. Os métodos de tratamento de dados, em particular dados pessoais, deverão ser avaliados e revisados a cada 6 (seis) meses pelo DPO e Operador de Dados, ou em período inferior, quando novos métodos, tecnologias, normativas ou política de boas práticas estiverem à disposição da **APTSJC**, nos termos do artigo 44, inciso III, da Lei Geral de Proteção de Dados.

11.5. Todos os dados pessoais e não pessoais mantidos pela **APTSJC** deverão ser revisados periodicamente, conforme estabelecido na Política de Retenção e Eliminação de Dados da Empresa.

11.6. O desempenho dos Usuários que lidam com dados pessoais deverá ser avaliado e revisado mensalmente, ou em período inferior, se necessário pelo DPO e o Operador de Dados, através de *softwares* específicos.

11.7. Todos os Usuários que lidam com dados pessoais serão obrigados a fazê-lo de acordo com os princípios e fundamentos dispostos na LGPD, bem como o Código de Ética e Conduta e todas as demais políticas da **APTSJC** aplicáveis, por contrato ou qualquer outro instrumento.

11.8. Nenhum dado, pessoal, poderá ser compartilhado informalmente e se um Usuário requerer acesso a quaisquer dados, pessoais, aos quais ele ainda não tenha acesso, tal acesso deverá ser formalmente solicitado ao DPO e respondido em consonância com o artigo 19, caput e incisos II, e artigo 41, § 2º, inciso I, da Lei Geral de Proteção de Dados.

11.9. Nenhum dado, pessoal ou não, pode ser transferido, ou de qualquer outro meio fornecido, a qualquer Usuário não autorizado, sem a autorização do Operador de Dados e DPO da **APTSJC.**

11.10. Todos os dados deverão ser manuseados com cuidado em todos os momentos e não deverão ser deixados sem supervisão ou à vista de Usuários não autorizados ou outras partes a qualquer momento.

12. SEGURANÇA DE ACESSO

12.1. Os privilégios de acesso para todos os Sistemas de TI e dados pessoais deverão ser determinados com base nos níveis de autoridade técnica dos Usuários dentro da **APTSJC** e nos requisitos de suas funções e cargos. Os Usuários não deverão ter acesso a quaisquer Sistemas de TI ou dados que não sejam razoavelmente necessários para o cumprimento de suas funções de trabalho.

12.2. Os acessos às áreas físicas dos servidores e redes da **APTSJC** devem ser restringidos e controlados. O registro deverá ser feito no servidor de log, quando aplicável, e o controle deverá ser realizado por, mas não se limitando a, crachás individuais ou por biometria.

12.3. Todos os Sistemas de TI, em particular os dispositivos móveis, incluindo, mas não se limitando a laptops e tablets, deverão ser criptografados e isolados, a fim de garantir que dados e informações importantes ligadas aos dados pessoais e à **APTSJC** sejam protegidos e, uma vez que sua finalidade tenha terminado, sejam prontamente eliminados.

12.4. Todos os Sistemas de TI, deverão ser protegidos contra malwares, incluindo, mas não se limitando a, *Ransomwares, Worms*, Cavalos de Tróia, *Spywares*, *Malwares*, *Adwares*, sendo a passivo de quaisquer mudanças por deliberação da **APTSJC.** A proteção contra malwares deverá ser realizada de maneira ininterrupta pelo Responsável de Tecnologia e Segurança da Informação da **APTSJC**, adotando-se ações de conscientização e proteção como:

a) Instalação e execução de programas e softwares anti-malware nos dispositivos móveis dos Usuários;

b) Utilização de programas e softwares que impeçam a instalação pelos Usuários de softwares sem o consentimento do Departamento de Tecnologia e Segurança da Informação da **APTSJC** ;

c) Utilização de programas e softwares nos dispositivos móveis dos Usuários que os impeçam de acessar determinados tipos de conteúdo;

d) Adoção de programa interno de conscientização a respeito dos perigos e formas de evitar a instalação de malwares em dispositivos móveis;

e) Manutenção de navegadores de Internet e seus complementos atualizados, bem como de atualizações e melhorias dos *endpoints* e *gateways* de rede; e

f) Impedir, na rede confiável, que sejam distribuídos e certificados sistemas antes de serem autorizados pelo Responsável de Tecnologia e Segurança da Informação.

§ Único: A lista indicada no item 12.4 é exemplificativa e não impede outras ações da APTSJC para atendimento no disposto deste item.

12.5. Todos os Sistemas de TI, em particular os dispositivos móveis, incluindo, mas não se limitando a laptops tablets, deverão ser protegidos com uma senha ou código de acesso seguro, ou qualquer outra forma de sistema de login seguro, que o Coordenador de TI aprove e considere apropriado. Nem todas as formas de login biométrico são consideradas seguras. Apenas os métodos aprovados pelo Responsável de Tecnologia e Segurança da Informação poderão ser usados.

12.6. Todas as senhas deverão estar de acordo com a futura política interna de senhas da organização e deverão, quando o software, sistema, site, computador ou dispositivo permitir:

a) Criação mediante a utilização de gerenciadores de senhas, resultando em senhas aleatórias e únicas (sempre que possível) para cada software, sistema, site, computador, dispositivo ou domínio de segurança;

b) Onde a utilização dos gerenciadores de senhas não for possível, utilizar uma combinação de letras, números e símbolos;

c) Não utilizar como senha, uma única palavra de qualquer dicionário existente, seja brasileiro ou estrangeiro, por exemplo: Password;

d) Não utilizar uma única palavra de qualquer dicionário existente, com alterações de caracteres, por exemplo: P4s5WorD;

e) Não utilizar misturas de informações pessoais ou de conhecimento público para criação das senhas, como datas comemorativas, nomes de familiares, nomes de animais, nomes memoráveis, eventos ou lugares etc.;

f) Em todos os casos, nunca utilizar senhas repetitivas ou sequenciais que são facilmente quebráveis. (Exemplos: 1234abcd, aaaaaaa, 123456, 123123, 321321 etc.);

g) Utilização de Autenticação Multifator (MFA), sempre que possível; e

h) Realização de trocas de senhas periodicamente conforme as políticas internas, bem como sempre que houver qualquer suspeita ou confirmação de possível vazamento.

12.7. As senhas deverão ser mantidas em sigilo por cada Usuário. Sob nenhuma circunstância um Usuário deve compartilhar sua senha com quaisquer terceiros, incluindo o Coordenador de TI e a equipe de TI. Nenhum Usuário terá sua senha legitimamente solicitada por ninguém, em nenhum momento, e qualquer solicitação desse tipo deve ser recusada. Se um Usuário tiver motivos para acreditar que outro indivíduo obteve sua senha, ele deve alterá-la imediatamente e relatar a suspeita de violação de segurança ao Responsável de Tecnologia e Segurança da Informação e, se os dados pessoais puderem ser acessados por um indivíduo não autorizado deverá incluir na notificação o DPO.

12.8. Se um Usuário esquecer sua senha, tal evento deverá ser relatado ao Responsável de Tecnologia e Segurança da Informação imediatamente.

12.9. O Departamento de Tecnologia da Informação tomará as providências necessárias para restabelecer o acesso do Usuário aos Sistemas de TI e informática, podendo incluir a emissão de uma senha temporária que poderá ser total ou parcialmente do conhecimento pelo responsável para resolução do problema. Uma nova senha deverá ser configurada pelo Usuário imediatamente após o restabelecimento do acesso aos Sistemas de TI e informática.

12.10. Os Usuários jamais deverão anotar senhas de modo físico. Caso um Usuário não se lembre de uma senha, ela deverá ser armazenada com segurança, por exemplo, em um cofre/banco de dados de senhas criptografado, através de indicação do Responsável de Tecnologia e Segurança da Informação. Em nenhuma circunstância as senhas devem ser deixadas em exibição para que

outros vejam, por exemplo, anexando uma nota à tela do computador, escrito em nota física ou armazenado em dispositivos particulares.

12.11. Todos os Sistemas de TI com visores deverão ser protegidos, com um bloqueio de tela protegido por login e senha, o qual será ativado após 3 (três) minutos de inatividade. É obrigatória a realização do bloqueio de tela manual pelo Usuário sempre que for se afastar ou se ausentar momentaneamente do ambiente do equipamento. A ativação do protetor de tela não interrompe ou interromperá quaisquer outras atividades que estejam ocorrendo no computador.

12.12. Todos os dispositivos móveis, incluindo, mas não se limitando a, laptops e tablets, fornecidos pela **APTSJC** deverão ser configurados para bloquear, após 3 (três) minutos de inatividade, exigindo login e senha, código de acesso, ou outra forma de login para desbloquear, despertar ou algo semelhante. Os Usuários não poderão alterar este período de tempo, salvo exceções devidamente homologadas pelo Coordenador de TI sendo ainda obrigatória a realização do bloqueio de tela manual pelo Usuário sempre que for se afastar ou se ausentar momentaneamente do ambiente do equipamento.

12.13. Os Usuários não podem usar nenhum software que permita o acesso de terceiros aos Sistemas de TI sem o consentimento expresso do Coordenador de TI. Qualquer software deve ser razoavelmente exigido pelo Usuário para o desempenho de sua função de trabalho e deve ser totalmente inspecionado e liberado pelo Coordenador de TI e, quando tal acesso torna os dados pessoais acessíveis por terceiros, também pelo DPO do **APTSJC**

12.14. Os Usuários, por regra, não poderão conectar seus próprios dispositivos particulares, incluindo, mas não se limitando a, laptops, tablets e smartphones, às redes da **APTSJC,** exceto em situações específicas e justificadas mediante a autorização formal pelo Coordenador de TI, em rede segregada SSID: PQTEC da **APTSJC**, após expressa autorização e liberação, bem como em observância às orientações específicas repassadas pelo respectivo departamento.

12.15. Todos os Sistemas de TI, dispositivos móveis, incluindo, mas não se limitando a laptops, tablets e smartphones, deverão passar por periódicos processos de

backups conforme a política de backups da organização, a serem armazenados em local seguro definido pelo Coordenador de TI da **APTSJC** O Coordenador de TI, também, será responsável por definir o método para realização do backup e garantir que o sistema de restauração está funcionando.

13. SEGURANÇA DE ARMAZENAMENTO DE DADOS

13.1. Todos os dados armazenados em formato eletrônico, e em particular dados pessoais, devem ser armazenados de forma segura usando senhas e criptografia de dados físicos devem ser rigorosamente catalogados e em um prazo de 12 (doze) meses, sendo necessário à sua digitalização e suas vias físicas destruídas, quando permitida a prática, que, respectivamente, realizam o tratamento de tais dados pessoais no interesse exclusivo da **APTSJC.**

13.2. Nenhum dado pessoal deve ser armazenado em qualquer dispositivo móvel, incluindo, mas não limitado a laptops, tablets e smartphones, sem que tal dispositivo pertença à **APTSJC** ou de outra forma sem a aprovação formal por escrito do DPO e, no caso de tal aprovação, estritamente de acordo com todas as instruções e limitações descritas quando a aprovação é concedida, e por um período não superior ao estritamente necessário.

13.3. Nenhum dado, e em particular dados pessoais, deve ser transferido para qualquer computador ou dispositivo que pertença pessoalmente a um Usuário, a menos que o Usuário em questão seja um contratante ou subcontratado trabalhando em nome da **APTSJC** e que o Usuário tenha concordado em cumprir integralmente todas as políticas de proteção de dados da **APTSJC** e diretrizes da LGPD, bem como mediante controle interno de acesso e transferência.

14. PROTEÇÃO DE DADOS

14.1. Todos os dados pessoais, em observância ao artigo 5º, inciso I, da Lei Geral de Proteção de Dados, tratados pela **APTSJC** serão estritamente tratados de acordo com os princípios da LGPD, e as disposições da futura Política de

Proteção de Dados da **APTSJC** bem como Código de Ética e Conduta e demais políticas aplicáveis.

14.2. Todos os Usuários que lidam com dados para e em nome da **APTSJC** estão sujeitos e devem cumprir as disposições da Política de Proteção de Dados, LGPD, Código de Ética e Conduta e demais políticas aplicáveis da **APTSJC**, em todos os momentos. Em particular, aplica-se o seguinte:

a) Todos os e-mails contendo dados pessoais e/ou outros dados cobertos por esta Política devem ser criptografados;

b) Todos os e-mails contendo dados pessoais e/ou outros dados cobertos por esta Política devem ser marcados como "confidenciais";

c) Os dados cobertos por esta Política podem ser transmitidos apenas por redes seguras; a transmissão em redes não seguras não é permitida em nenhuma circunstância;

d) Os dados cobertos por esta Política não podem ser transmitidos por uma rede sem fio sem a utilização obrigatória do acesso a VPN configurado pelo Responsável de Tecnologia e Segurança da Informação;

e) Todos os dados pessoais abrangidos por esta Política a serem transferidos fisicamente, inclusive em meio eletrônico removível, deverão ser transferidos em recipiente adequado marcado como "confidencial"; e

f) Quando quaisquer dados cobertos por esta Política forem visualizados em uma tela de computador e este for deixado sem supervisão por qualquer período, o Usuário deverá bloquear o computador e a tela antes de deixá-los.

14.3. Quaisquer questões relacionadas com a proteção de dados pessoais devem ser encaminhadas para o DPO da **APTSJC .**

Nome: Caroline Cubas Lopes – Assessora Jurídica

E-mail: lgpd@pqtec.org.br

15. EXCLUSÃO E ELIMINAÇÃO DE DADOS

15.1. Quando quaisquer informações e dados, e em particular dados pessoais, devam ser apagados ou de outra forma eliminados, nos termos do artigo 5º,

inciso XIV, da Lei Geral de Proteção de Dados, por qualquer motivo – incluindo quando as cópias foram feitas e não são mais necessárias –, os dados e as informações devem ser excluídos e/ou descartados com segurança, utilizando equipamentos de fragmentação de papeis para documentos e informações em formato físico, sendo que os dispositivos de armazenamento físicos, as mídias removíveis como Pendrives, HDs, Notebooks, etc., deverão ser entregues ao Responsável de Tecnologia e Segurança da Informação para que ele realize o *wipe* de todas, ou seja, fazer a limpeza de todo o conteúdo existente nesses dispositivos antes de realizar o descarte do dispositivo. O descarte apropriado desses dispositivos deve ser feito através de empresa especializada para tal finalidade.

15.2. Para a eliminação de informações em meio digital, deverá ser consultado o Responsável de Tecnologia e Segurança da Informação para orientações, bem como as políticas vigentes da **APTSJC** para que seja feito o descarte apropriado dos dados.

15.3. É proibida a reutilização de papeis impressos com dados sensíveis ou dados pessoais, para finalidade de rascunho, devendo ser imediatamente fragmentados ou tornados inúteis caso não sejam mais utilizados;

16. USO DA INTERNET E DO E-MAIL

16.1. Todos os Usuários devem cumprir as disposições das políticas de comunicações, e-mails e Internet da **APTSJC** ao utilizarem os Sistemas de TI da organização.

16.2. Quando as disposições desta Política exigirem que quaisquer medidas adicionais sejam tomadas para garantir a segurança ao usar a Internet ou e-mail, além dos requisitos impostos pela política de comunicações, e-mail e Internet, os Usuários deverão tomar todas as medidas necessárias e de segurança dispostas na referida política e demais políticas da **APTSJC** relacionadas à proteção de dados.

17. RELATANDO VIOLAÇÕES DE SEGURANÇA

17.1. Todas as preocupações, dúvidas, suspeitas de violação ou violações conhecidas que se relacionam aos Sistemas de TI devem ser encaminhadas imediatamente ao Operador de dados da **APTSJC.**

17.2. Todas as preocupações, perguntas, suspeitas de violações conhecidas relacionadas a outros dados cobertos por esta Política devem ser encaminhadas imediatamente para o DPO da **APTSJC**, informando: local e data, ou suspeita, da violação; indicar se a violação ainda está em ação; breve descrição sobre os dados pessoais e informações afetadas; e circunstâncias em que ocorreu a violação.

17.3. Ao receber uma pergunta ou notificação de uma violação, o indivíduo ou departamento responsável deve, dentro de 24 (vinte e quatro) horas, avaliar a questão incluindo, mas não se limitando a, determinar probabilidade, impacto e nível de risco associado a ela, e devem ser tomadas todas e quaisquer medidas consideradas necessárias para responder à questão de forma imediata e efetiva.

17.4. Sob nenhuma circunstância um Usuário deve tentar resolver uma violação de segurança por conta própria, nos termos do item 17.2 desta Política.

17.5. Todas as violações de segurança, de qualquer forma corrigidas, devem ser documentadas, devendo o DPO da **APTSJC** atuar em conjunto com os Usuários para obter as informações necessárias para solucionar o incidente de segurança ou violação de dados, mitigar danos aos titulares de dados e, a depender da gravidade, comunicar a Autoridade Nacional de Proteção de Dados (ANPD) e os titulares de dados, nos termos do artigo 48, caput, § 1º e incisos, da LGPD.

18. PENALIDADES

18.1. O descumprimento ou violação das regras previstas nesta Política e demais documentos em vigor poderá resultar na aplicação das sanções previstas em procedimentos internos, contratos e legislação vigente.

18.2. O responsável pela violação ou descumprimento, responderá disciplinarmente, civilmente ou criminalmente pelo prejuízo que vier a ocasionar à **APTSJC,**

podendo resultar em desligamento, rescisão de contrato de prestação de serviços e eventuais processos judiciais, quando cabíveis.

19. REVISÃO DA POLÍTICA

A **APTSJC** deverá revisar esta Política pelo menos a cada 1 (um) ano e, conforme necessário, a fim de garantir que ela permaneça atualizada e adequada para seu propósito. Todas as perguntas, preocupações e outros comentários relacionados a esta Política devem ser comunicados ao Operador de Dados, bem como ao DPO, quando apropriado.

20. IMPLEMENTAÇÃO DA POLÍTICA

Esta Política será considerada efetiva na data de sua publicação. Nenhuma parte desta Política terá efeito retroativo e, portanto, se aplicará apenas a questões que ocorram durante seu período de vigência, até que superveniente revisão a substitua.

ASSOCIAÇÃO PARQUE TECNOLOGICO DE SÃO JOSE DOS CAMPOS

Jeferson de Lima Cheriegate

Diretor Geral