POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

ÍNDICE

1. OBJETIVO

Este documento tem por objetivo estabelecer diretrizes, definições, restrições e requisitos de segurança da informação, adotados pelo TENIS CLUBE PAULISTA. Tais diretrizes fundamentam as normas e procedimentos de segurança da informação implementados, inclusive cumpre requisitos da Lei Geral de Proteção de Dados.

Para o cumprimento da finalidade supracitada são estabelecidos na política de segurança da informação do TÊNIS CLUBE PAULISTA os objetivos a seguir:

- Definir o escopo da segurança da informação para a empresa e filiais ou outras unidades do TÊNIS CLUBE PAULISTA;
- Orientar, por meio de suas diretrizes, todas as ações de segurança da informação, objetivando reduzir riscos e garantir a integridade, sigilo e disponibilidade das informações de acordo com os requisitos do negócio e com as leis e regulamentações relevantes;
- Permitir a adoção de soluções de segurança da informação integradas;
- Servir de referência para auditoria interna e externa.

2. APLICAÇÃO

2.1. Geral

2.1.1. Ativos de Informação e ativos de processamento de dados do TÊNIS CLUBE PAULISTA;

2.1.2. Ativos de processamento de colaboradores, terceiros e prestadores de serviços que sejam conectados à rede corporativa do TÊNIS CLUBE PAULISTA.

2.2. Áreas de Negócio

2.2.1. Todas as áreas de negócio da empresa e filiais do TÊNIS CLUBE PAULISTA.

2.3. Público-alvo

2.3.1. Colaboradores;

2.3.2. Terceiros e Prestadores de Serviços.

2.4. Política de Segurança da Informação

2.4.1. Senhas de Acesso;

2.4.2. Acesso à Internet;

2.4.3. E-mail;

2.4.4. Servidor de Arquivos (armazenamento de arquivos);

2.4.5. Instalação e utilização de softwares;

2.4.6. Desenvolvimento de softwares específicos;

2.4.7. Utilização de equipamentos de informática;

2.4.8. Dispositivos móveis;

2.4.9. Provisionamento de acesso a sistemas e serviços de TI;

2.4.10. Política de segurança dos sistemas.

3. DEFINIÇÕES

3.1. Siglas

3.1.1. PSI – Política de Segurança da Informação;

3.1.2. TI – Tecnologia da Informação;

3.1.3. SI – Sistemas da Informação;

3.1.4. ISO – International Organization for Standardization;

3.1.5. ERP – Enterprise Resource Planning;

3.1.6. SGSI – Sistema de Gestão de Segurança da Informação;

3.1.7. DPO – Data Protector Officer (Encarregado)

3.2. TERMINOLOGIA

3.2.1. ISO/IEC17799 – Norma de segurança da informação revisada em 2005 pela Organização Internacional para Padronização (ISO) e pela Comissão Eletrônica Internacional (IEC). O padrão é um conjunto de recomendações para prática de gestão em segurança da informação. A ISO/IEC17799 tem como objetivo principal, zelar pela confidencialidade, integridade e disponibilidade das informações;

3.2.2. Informação – É um ativo essencial para os negócios de uma organização e consequentemente necessita ser adequadamente protegido;

3.2.3. Segurança da Informação – Conforme a norma NBR ISO/IEC17799, a segurança da informação é caracterizada pela preservação dos três atributos básicos da informação:

- Confidencialidade: é a garantia de que a informação não seja disponível ou revelada a indivíduos, entidades ou processos não autorizados;
- Integridade: é a proteção da exatidão e completeza da informação e dos métodos de processamento;
- Disponibilidade: é a garantia de que as pessoas autorizadas tenham acesso às informações, bem como aos bens associados, quando requeridos.

3.2.4. Ativo – Tudo o que tem valor para a organização;

3.2.5. Ativo de Informação – Patrimônio composto por todos dados e informações geradas e manipuladas durante a execução dos sistemas e processos;

3.2.6. Ativo de Processamento - Patrimônio composto por todos os elementos de hardware e software necessários para a execução dos sistemas e processos;

3.2.7. Política de Segurança – Conjunto de diretrizes destinadas a definir a proteção adequada dos ativos produzidos pelos Sistemas de Informação;

3.2.8. Controles de Acesso – São restrições relacionadas ao acesso às informações dos sistemas e/ou aplicativos;

3.2.9. Direito de Acesso – Privilégio associado a um cargo, pessoa ou processo para ter acesso a um ativo;

3.2.10. Ferramentas – Conjunto de processos, procedimentos, normas, hardware, software e demais recursos, por meio das quais se aplica a Política de Segurança da Informação;

3.2.11. Incidente de segurança – Qualquer evento ou ocorrência que promova uma ou mais ações que comprometa ou que seja uma ameaça à integridade, autenticidade, ou disponibilidade de qualquer ativo relacionado à Segurança da Informação, como exemplo:

- Tentativas de ganhar acessos não autorizados a sistemas ou pastas/dados;
- Ataques de negação de serviço;
- Uso ou acesso não autorizado a um sistema aplicativo;
- Modificações em um sistema, sem o conhecimento, instruções ou consentimento prévio da gerência de T.I.;
- O não cumprimento (desrespeito) a política de segurança;

3.2.12. Proteção dos ativos – Processos pelo qual os ativos devem receber classificação quanto ao grau de sensibilidade. O meio de registro de um ativo de informação deve receber a mesma classificação de proteção dada ao ativo que o contém;

3.2.13. Responsabilidade – Obrigações e deveres da pessoa que ocupa determinada função em relação ao acervo de informações;

3.2.14. Senha Fraca ou Óbvia – Utilização de caracteres de fácil associação com o dono da senha (usuário), ou que seja muito simples ou pequena, tais como os exemplos abaixo:

- Datas de aniversário, casamento, nascimento;
- O próprio nome, nome de familiares;
- Sequencias numéricas simples;
- Sequência particulares do teclado (ex.: ASDFG);

3.2.15. Log de dados – Em computação, Log de dados é o termo utilizado para descrever o processo de registro de eventos relevantes em um sistema computacional. Esses registros podem ser utilizados para restabelecer o estado original de um sistema ou para que um administrador conheça seu comportamento no passado. Um arquivo de log pode ser utilizado também para auditoria e diagnóstico de problemas em sistemas computacionais;

3.2.16. Tecnologia da Informação (TI) – Integração e gestão de recursos de hardware e software destinadas à captura, processamento, armazenamento e comunicação de dados, visando automatizar a produção e gestão das informações;

3.2.17. ERP – Enterprise Resource Planning – Sistemas integrados de gestão empresarial. São sistemas de informação que integram todos os dados e processos de uma organização em um único sistema. A integração pode ser funcional (sistemas de finanças, contabilidade, recursos humanos, marketing, vendas etc.) ou sistêmica (sistema de processamento de transações, de informações gerenciais, de apoio à decisão etc.);

3.2.18. Compliance – Significa agir de acordo com uma regra, um pedido ou um comando. Dentre os principais objetivos das normas de compliance estão à prevenção e o combate a fraudes, a criação e o monitoramento do cumprimento de manuais e normas internas, controles internos e cultura organizacional;

3.2.19. Backup – Cópia de dados de um dispositivo para o outro com o objetivo de posteriormente, recuperá-los em casos de necessidade (como quando há algum problema com os dados originais);

3.2.20. PDCA – também chamado de Ciclo de Deming ou Ciclo de Shewhart, é uma ferramenta de gestão que tem como objetivo promover a melhoria contínua dos processos por meio de um circuito de quatro ações: Plan (planejar), Do (fazer), Check (checar) e Act (agir);

- Planejar: estabelecer a política de segurança da informação, objetivos, processos e procedimentos do SGSI (sistema de gestão de segurança da informação), relevantes para a gestão de riscos e a melhoria da segurança da

informação para produzir resultados de acordo com as políticas e objetivos globais de uma organização;

- Fazer: implementar e operar a política, controles, processos e procedimentos do SGSI;
- Checar: avaliar e, quando aplicável, medir o desempenho de um processo frente à política, objetivos e experiência prática do SGSI e apresentar os resultados para análise crítica pela direção;
- Agir: executar as ações corretivas e preventivas, com base nos resultados da auditoria interna do SGSI e da análise crítica pela direção ou outra informação pertinente, para alcançar a melhoria contínua do SGSI;

3.2.21. Risco – Perigo ou possibilidade de perigo, ou seja, é a probabilidade de acontecer algo pela exploração das vulnerabilidades de um determinado ambiente, provocando possíveis problemas financeiros e impactos nos negócios;

3.2.22. Risco residual – Risco remanescente após o tratamento do risco inicial;

3.2.23. Vulnerabilidade – Fraqueza que é associada ao ativo da organização e que caso explorado por uma ameaça, pode representar riscos a organização.

Também pode ser definida como sendo o ponto onde o sistema poderá ser suscetível a ataques;

3.2.24. Gestão de identidade – Gerenciamento do ciclo de vida do usuário de TI.

3.2.25. Lei Geral de Proteção de Dados (LGPD) – Sancionada em agosto de 2018. A LGPD estabelece regras sobre coleta, armazenamento, tratamento e compartilhamento de dados pessoais, impondo mais proteção e penalidades para o não cumprimento.

4. REFERÊNCIAS

XXXXX - Termo guarda e conservação de notebook e acessórios

YYYYYY - Formulário de Desenvolvimento Específico

ZZZZZ – Ficha do Usuário

FE0004 - Termo de Entrega de Dispositivos Móveis

HELPDESK: Sistema de abertura para atendimento Técnico

ISO/IEC 17799: Norma internacional de segurança da informação

NBR ISO/IEC 17799: Versão Brasileira da norma ISO/IEC 17799

ISO/IEC 27001: Prover um modelo para estabelecer, implementar, operar, manter, monitorar e melhorar um Sistema de Gestão de Segurança da Informação (SGSI)

NBR ISO/IEC 27001: Versão brasileira da norma ISO/IEC 27001

NBR ISO/IEC 27002:2005: Versão brasileira da norma ISO/IEC 27002

Lei 13709/2018: Lei Geral de Proteção de Dados Pessoais (LGPD)

COBIT Framework 4.1: Objetivos de Controles relacionados aos usos da TI

ITIL: Information Technology Infrastructure Library (biblioteca de infraestrutura de TI). Conjunto de melhores práticas para a gestão de serviços em TI.

5. DIRETRIZES

5.1. GERAIS

5.1.1. A Política de Segurança da Informação do TÊNIS CLUBE PAULISTA se aplica a todos os seus recursos humanos e tecnológicos. A abrangência dos recursos citados refere-se tanto àqueles ligados a ela em caráter permanente quanto temporário;

5.1.2. No que se refere à segurança da informação, considere-se proibido tudo que não esteja previamente autorizado pela área de T.I.;

5.1.3. Novos sistemas aplicativos, assim como todos os novos ativos de informação e ativos de processamento, devem ser adquiridos, implementados

e/ou desenvolvidos, somente após a prévia autorização da área de TI e considerar os requisitos mínimos de segurança da informação;

Esta política de segurança da informação deve ser considerada como subsídio essencial para o desenvolvimento de processos de aquisição de bens e serviços de Tecnologia da Informação;

5.1.4. Novos projetos de implantação de sistemas de informação e softwares de uso geral, deve respeitar as regras de segurança estabelecidas neste procedimento;

5.1.5. Todos os sistemas implantados e que não estejam em conformidade com esta PSI, devem ser ajustados, adequando-se as regras e controles de segurança da informação descritos nesta PSI;

5.1.6. A informação é protegida de acordo com o seu valor e criticidade, considerando o nível dos atributos: confidencialidade, integridade e disponibilidade;

5.1.7. As informações de propriedade do TÊNIS CLUBE PAULISTA, devem ser de uso restrito para os fins a que se destinam, não podendo, de forma alguma, sob nenhum propósito, serem apropriadas por usuários (colaboradores, terceiros e prestadores de serviço);

5.1.8. A identificação do usuário por meio de crachá, senha ou outro meio de identificação, é pessoal e intransferível, qualificando-o como responsável por todas as atividades desenvolvidas através dela.

É pré-requisito para a liberação do uso de qualquer uma dessas formas de identificação, a assinatura do Termo de Responsabilidade no Uso de Recursos de Tecnologia da Informação – XXXXX, que comprove sua ciência às condições de uso, seus direitos e deveres quanto ao acesso dos recursos computacionais da empresa e filiais do TÊNIS CLUBE PAULISTA;

5.1.9. O cumprimento da PSI será acompanhado e auditado pela área de TI a qual se reserva o direito de monitorar o tráfego de informações, incluindo o acesso à internet, uso do correio eletrônico e sistemas aplicativos;

5.1.10. Todos os usuários, ao tomarem conhecimento de qualquer incidente de segurança da informação devem notificar o fato imediatamente para a área de T.I., para que esta tome as providências cabíveis;

5.1.11. Todos os usuários em geral devem ter acesso liberado apenas aos recursos mínimos necessários à execução de suas tarefas, de forma a evitar vulnerabilidades às informações;

5.1.12. Somente atividades lícitas, éticas e administrativamente admitidas, devem ser realizadas pelos usuários em geral, quando da utilização dos recursos computacionais do TÊNIS CLUBE PAULISTA, ficando os transgressores sujeitos às penalidades vigentes;

5.1.13. Somente colaboradores vinculados à área de desenvolvimento de software (área de Sistemas), poderão desenvolver programas. Em casos excepcionais a área de negócio envolvida deverá preencher o Formulário de Desenvolvimento Específico – YYYYYY e encaminhar para a área de TI para análise e posterior autorização/recusa;

5.1.14. Programas e documentos desenvolvidos por colaboradores e prestadores de serviço são de propriedade do TÊNIS CLUBE PAULISTA, salvo em casos expressamente assegurados por contrato formal;

5.1.15. Para a uniformidade da informação, a PSI deverá ser comunicada a todos os colaboradores, terceiros e prestadores de serviço do TÊNIS CLUBE PAULISTA, a fim de que a política seja cumprida dentro e fora da empresa;

5.1.16. Deverá constar nos contratos do TÊNIS CLUBE PAULISTA o anexo de Acordo de Confidencialidade ou cláusula de Confidencialidade, como condição imprescindível para que possa ser concedido o acesso aos ativos de informação disponibilizados pela empresa;

5.1.17. Tanto a PSI quanto as normas deverão ser revistas e atualizadas periodicamente, sempre que algum fato relevante ou evento motive sua revisão;

5.1.18. Deverão ser criados e instituídos controles apropriados (recursos para), trilhas de auditoria ou registros de atividades, para sistemas de informação e de controle de ativos de informática em que a empresa julgar necessário

administrar riscos. Por questões de limitação de infraestrutura, trilhas de auditoria são ativadas sob demanda de processo de investigação;

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

5.1.20. O TÊNIS CLUBE PAULISTA exonera-se de toda e qualquer responsabilidade decorrente do uso indevido, negligente ou imprudente dos recursos e serviços concedidos aos seus colaboradores, reservando-se o direito de analisar dados e evidências para obtenção de provas a serem utilizadas nos processos investigatórios, bem como adotar as medidas legais cabíveis;

5.1.21. Esta PSI será implementada no TÊNIS CLUBE PAULISTA por meio de procedimentos específicos, obrigatórios para todos os colaboradores, independentemente do nível hierárquico ou função na empresa, bem como de vínculo empregatício ou prestação de serviço. O não cumprimento dos requisitos nesta PSI e das Normas de Segurança da Informação, acarretará violação às regras internas da empresa e sujeitará o usuário às medidas administrativas e legais cabíveis.

5.1.22. Todas as informações recebidas pela área de T.I. referente a vazamento de dados pessoais, devem ser direcionados ou comunicados ao DPO do TÊNIS CLUBE PAULISTA.

5.2. PENALIDADES/SANÇÕES

5.2.1. A não observância das regras desta Política de Segurança da Informação implicará na aplicação de penalidades administrativas, trabalhistas, cíveis e penais pela legislação vigente;

5.2.2. Política de senhas de acesso à rede:

- Tamanho mínimo: 8 caracteres;
- Complexidade: sem restrição;
- Tempo de expiração: 45 dias;

- Bloqueio de acesso por tentativas inválidas: acima de 5 tentativas erradas;
- Não repetição: das 6 últimas senhas usadas;
- Tempo de Bloqueio: 20 minutos, antes disso apenas através de solicitação ao departamento de TI;
- Confirmação de identidade para desbloqueio de senha: se um usuário ligar para o suporte pedindo o desbloqueio da senha, será verificado o nome do usuário, nome do gestor, departamento e matrícula, além de alguns dados aleatórios.
- Tempo mínimo de validade da senha: 3 dias de uso, antes disso, somente por intervenção do TI
- A senha é particular e intransferível, não podendo ser divulgada pelo mesmo a qualquer outra pessoa;
- No caso de suspeita de quebra de sigilo da senha, o colaborador deverá comunicar imediatamente o departamento de TI, solicitando a troca imediata da senha de acesso;
- Os dispositivos de identificação e senhas protegem a identidade do colaborador, evitando e prevenindo que uma pessoa se faça passar por outra perante o TÊNIS CLUBE PAULISTA e/ou terceiros;
- O uso dos dispositivos e/ou senhas de identificação de outra pessoa constitui crime tipificado no Código Penal Brasileiro (art. 307 – falsa identidade);
- Todos os dispositivos de identificação utilizados no TENIS CLUBE PAULISTA, como o número de registro do colaborador, o crachá, as identificações de acesso aos sistemas, os certificados e assinaturas digitais e os dados biométricos, têm de estar associados a uma pessoa física e atrelados inequivocamente aos seus documentos oficiais reconhecidos pela legislação brasileira;
- O usuário, vinculado a tais dispositivos identificadores, será responsável pelo seu uso correto perante o TÊNIS CLUBE PAULISTA e a legislação (cível, criminal e trabalhista);
- Todo e qualquer dispositivo de identificação pessoal, portanto, não poderá ser compartilhado com outras pessoas em nenhuma hipótese;

- Se existir login de uso compartilhado por mais de um colaborador, a responsabilidade perante o TÊNIS CLUBE PAULISTA e a legislação (cível, criminal e trabalhista) será dos usuários que dele se utilizarem. Somente se for identificado conhecimento ou solicitação do gestor de uso compartilhado ele deverá ser responsabilizado;
- O departamento de Recursos Humanos do TÊNIS CLUBE PAULISTA é o responsável pela emissão e pelo controle dos documentos físicos de identidade dos colaboradores;
- O departamento de TI responde pela criação da identidade lógica dos colaboradores do TÊNIS CLUBE PAULISTA, nos termos do formulário da Ficha de Usuário - ZZZZZ anexado a um chamado no sistema de Helpdesk solicitando seu cadastro;
- É de responsabilidade do gestor da área solicitante, indicar os recursos a serem liberados para seus respectivos colaboradores e/ou terceiros sob a sua responsabilidade;
- Devem ser distintamente identificados os visitantes, estagiários, empregados temporários, empregados regulares e prestadores de serviços, sejam eles pessoas físicas e/ou jurídicas. Ao realizar o primeiro acesso ao ambiente de rede local, o usuário deverá trocar imediatamente a sua senha, conforme as orientações apresentadas nesse procedimento;
- Os usuários com perfil de administrador ou acesso privilegiado, deverão utilizar uma senha de no mínimo 10 (dez) caracteres, alfanumérica, utilizando caracteres especiais (@ # $ %) e variação de caixa (maiúsculo e minúsculo), obrigatoriamente;
- É de responsabilidade de cada usuário a memorização de sua própria senha, bem como a proteção e a guarda dos dispositivos de identificação que lhe forem designados;
- As senhas não devem ser anotadas ou armazenadas em arquivos eletrônicos (Word, Excel, etc.), compreensíveis por linguagem humana (não criptografados), não devem ser baseados em informações pessoais;

- Os usuários podem alterar a sua própria senha, e devem ser orientados a fazê-lo, caso suspeitem que terceiros obtiveram acesso indevido ao seu login/senha;
- Todos os acessos devem ser imediatamente bloqueados (inativados) quando se tornarem desnecessários, portanto, assim que algum usuário for demitido ou solicitar demissão, o departamento de R.H. deverá imediatamente comunicar tal fato ao departamento de TI, a fim que essa providência seja tomada. A mesma conduta se aplica aos usuários cujo contrato ou prestação de serviços tenha se encerrado, bem como aos usuários de testes e outras situações similares;
- Caso o colaborador esqueça sua senha, ele deverá requisitar formalmente a troca ou comparecer à área de TI, onde receberá uma senha temporária que deverá ser alterada no primeiro acesso do colaborador;
- Em caso de necessidade de acesso por um fornecedor de software ou hardware aos sistemas computacionais da empresa, liberações de acesso remoto serão concedidas de forma controlada, por tempo determinado e sob supervisão da área de TI., que deve se orientar com DPO no caso de acesso a dados pessoais. Exceção aos fornecedores que tenham contrato com responsabilização sobre a gestão de ambientes sistêmicos, sempre sendo garantido o acesso com contas de usuários devidamente identificadas, perfis de acesso restritos as atividades inerentes aos contratos;
- É proibido o uso compartilhado de Login e senha nas funções de administração de sistemas e infraestrutura de TI no que tange a servidores, banco de dados e seus sistemas de controle e operação;

5.2.3. Proteção de telas (descanso de tela quando o computador fica sem interação do usuário)

- Após um curto período sem uso do monitor o mesmo é desligado, exceção feita a monitores/TV que atendem sistemas de TV Indoor, Oficinas, servidores dos postos, entre outros onde o mesmo necessita operar em regime de 24x7.

5.2.4. Papel de parede (imagem de fundo de tela quando o computador está ligado)

- É de responsabilidade do departamento de Marketing enviar o arquivo de papel de parede para a área de TI disponibilizá-lo nas estações;
- É proibido ao usuário alterar o papel de parede.

5.3. INTERNET

5.3.1. O acesso à Internet é para uso exclusivo de assuntos pertinentes à empresa;

5.3.2. É terminantemente proibido o acesso a páginas/sites de conteúdo pornográfico e suas derivações;

5.3.3. Todas as regras atuais do TÊNIS CLUBE PAULISTA visam basicamente o desenvolvimento de um comportamento eminentemente ético e profissional do uso da internet. Embora a conexão direta e permanente da rede corporativa da empresa com a internet ofereça um grande potencial de benefícios, ela abre a porta para riscos significativos para os ativos de informação;

5.3.4. Qualquer informação que é acessada, transmitida, recebida ou produzida na internet está sujeita a divulgação e auditoria, portanto o TENIS CLUBE PAULISTA em total conformidade legal, reserva-se o direito de monitorar e registrar todos os acessos a ela;

5.3.5. Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet são de propriedade da empresa, que pode analisar e, se necessário, bloquear qualquer arquivo, site, correio eletrônico, domínio ou aplicação armazenados na rede/internet, estejam eles em disco local, na estação de trabalho ou em áreas privadas da rede, visando assegurar o cumprimento de sua Política de Segurança da Informação;

5.3.6. O TENIS CLUBE PAULISTA, ao monitorar a rede interna, pretende garantir a integridade dos dados e programas. Toda tentativa de alteração dos parâmetros de segurança, por qualquer colaborador, sem o devido

credenciamento e a autorização para tal, será julgada inadequada e os riscos relacionados serão informados ao colaborador e ao respectivo gestor do setor e ao DPO. O uso de qualquer recurso para atividades ilícitas poderá acarretar as ações administrativas e as penalidades decorrentes de processos civil e criminal, sendo que nesses casos a empresa cooperará ativamente com as autoridades competentes;

5.3.7. Somente os colaboradores que estão devidamente autorizados a falar em nome do TÊNIS CLUBE PAULISTA para os meios de comunicação, poderão manifestar-se, seja por e-mail, entrevista on-line, podcast, seja por documento físico, entre outros. Apenas os colaboradores autorizados pelo TÊNIS CLUBE PAULISTA poderão copiar, captar, imprimir ou enviar imagens da tela para terceiros, devendo atender à norma interna de uso de imagens, à Lei de Direitos Autorais, à proteção da imagem garantida pela Constituição Federal, à Lei Geral de Proteção de Dados Pessoais e demais dispositivos legais;

5.3.8. É proibida a divulgação e/ou compartilhamento indevidos de informações em listas de discussão, sites ou comunidades de relacionamento, salas de bate-papo ou chat, comunicadores instantâneos ou qualquer outra tecnologia correlata que venha a surgir na internet;

5.3.9. O uso, instalação, cópia ou distribuição não autorizada de softwares que tenham direitos autorais, marca registrada ou patente na internet, são expressamente proibidos. Qualquer software não autorizado baixado, será excluído pela área de TI e o responsável pelo ato, devidamente advertido;

5.3.10. Os colaboradores não poderão em hipótese alguma utilizar os recursos do TÊNIS CLUBE PAULISTA para fazer o download ou distribuição de software ou dados pirateados, atividade considerada delituosa de acordo com a legislação nacional;

5.3.11. A utilização de programas WEB específicos (SPED, conectividades sociais, redes de relacionamento etc.), poderão ser utilizados por usuários que tenham atividades profissionais relacionadas a essas necessidades, mediante solicitação do gestor da área solicitante;

5.3.12. Como regra geral, materiais de cunho sexual não poderão ser expostos, armazenados, distribuídos, editados, impressos ou gravados por meio de quaisquer recursos;

5.3.13. Colaboradores com acesso à internet não poderão efetuar upload (subida) de qualquer software licenciado o TÊNIS CLUBE PAULISTA ou de dados de sua propriedade aos seus parceiros e clientes, sem expressa autorização do responsável pelo software ou pelos dados;

5.3.14. Os colaboradores não poderão utilizar os recursos do TÊNIS CLUBE PAULISTA para deliberadamente propagar qualquer tipo de vírus, worm, cavalo de troia, spam, assédio, perturbação ou programas de controle de outros computadores;

5.3.15. O acesso a softwares peer-to-peer (Kazaa, Dreamule, Bit Torrent e afins), não serão permitidos. Já os serviços de streaming (canais de broadcast e afins) e os serviços de comunicação instantânea (MSN, SKYPE e afins), serão permitidos a grupos específicos, devidamente autorizados e poderão ser bloqueados caso o gestor requisite formalmente à área de TI. Sites de streaming de rádio são também proibidos de acesso.

5.3.16. O acesso a conteúdo bloqueado será liberado mediante a abertura de chamado no sistema de Helpdesk, análise de segurança da informação, aprovação dos gestores envolvidos, aprovação do gestor de TI e do DPO em caso de dados pessoais;

5.3.17. Não é permitido acesso a sites de proxy;

5.3.18. Não é permitido aos usuários com acesso à Internet, extraírem (download) de arquivos ou programas com características que representem risco a segurança, como: arquivos compactados, programas executáveis, scripts, arquivos de música ou vídeo, ou similares. Caso haja real necessidade de fazê-lo, o usuário deverá solicitar essa operação ao departamento de TI, por meio de um chamado no sistema de Helpdesk;

5.3.19. O recurso de download é proibido aos usuários da empresa. Quando houver necessidade de download de qualquer arquivo, o usuário deve

procurar o departamento de TI para que o mesmo análise, e em caso de concordância, efetue o download.

5.3.20. Em caso de necessidade de acesso à Internet para visitantes ou prestadores de serviços, o responsável pelo referido, deverá solicitar ao depto. de TI a configuração do equipamento e liberação do acesso.

5.3.21. É indispensável, informar ao DPO quando o procedimento envolver dados pessoais por qualquer departamento.

5.4. E-MAIL

5.4.1. A utilização do e-mail é restrita a assuntos da organização, sendo proibida também para:

- Enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionados a uso legitimo da empresa;
- Enviar mensagens por correio eletrônico pelo endereço que torne seu remetente e/ou o TÊNIS CLUBE PAULISTA ou suas coligadas, vulneráveis a ações civis ou criminais;
- Divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins, sem autorização expressa e formal concedida pelo proprietário desse ativo de informação;
- Falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários, com o objetivo de evitar as punições previstas;
- Apagar mensagens pertinentes de correio eletrônico quando qualquer uma das empresas do TÊNIS CLUBE PAULISTA estiver sujeita a algum tipo de investigação;
- Produzir, transmitir ou divulgar mensagem que:
- Contenha qualquer ato ou forneça orientação que conflite ou contrarie os interesses do TÊNIS CLUBE PAULISTA;
- Contenha ameaças eletrônicas, como: spam, mail bombing, scripts, links duvidosos e vírus de computador;

- Contenha arquivos com código executável ou qualquer outra categoria de código que represente um risco à segurança;
- Vise obter acesso não autorizado a outro computador, servidor ou rede;
- Vise interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
- Vise burlar qualquer sistema de segurança;
- Vise vigiar secretamente ou assediar outro usuário;
- Vise acessar informações confidenciais sem explicita autorização do proprietário;
- Vise acessar indevidamente informações que possam causar prejuízos a qualquer pessoa;
- Inclua imagens criptografadas ou de qualquer forma mascaradas;
- Contenha anexo(s) superior(es) a 10MB para envio (interno ou externo);
- Tenha conteúdo considerado impróprio, obsceno ou ilegal;
- Seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico entre outros;
- Contenha perseguição preconceituosa baseada em sexo, raça, incapacidade física ou mental;
- Tenha fins políticos locais ou do país (propaganda política);
- Inclua material protegido por direitos autorais sem a permissão do detentor dos direitos;

5.4.2. As mensagens de correio eletrônico sempre deverão incluir assinatura com formato pré-definido pelo TENIS CLUBE PAULISTA, sob a responsabilidade do departamento de Marketing;

5.4.3. Todo colaborador do TÊNIS CLUBE PAULISTA ou prestador de serviço deverá garantir a limpeza periódica de sua caixa de correio eletrônico, deixando-a com o tamanho máximo de 1GB, tamanho este máximo recomendado pelo fabricante do Microsoft Outlook;

5.4.4. É proibido a troca de informações de dados pessoais de colaboradores ou de terceiros sem o conhecimento do DPO.

5.5. SERVIDOR DE ARQUIVOS (ARMAZENAMENTO DE ARQUIVOS)

5.5.1. É terminantemente proibido o armazenamento de arquivos não pertencentes à empresa, tais como: formulários ou qualquer documento que contenha dados pessoais, normas, fotos, vídeos, e filmes no servidor de arquivos;

5.5.2. É proibido o armazenamento de arquivos particulares, protegidos por senha, criptografia, ou qualquer outro tipo que contrarie as regras descritas nesta PSI e que venham a impedir e/ou dificultar possíveis auditorias de conteúdo;

5.5.3. Todos os arquivos devem ser armazenados no servidor de arquivos e nunca nas estações de trabalho;

5.5.4. O único arquivo mantido nas estações é o do serviço de correio eletrônico. Este arquivo contém todo o histórico de e-mails do usuário. É de responsabilidade do usuário fazer a cópia de segurança deste arquivo para sua área específica no servidor de arquivos, a fim deste fazer parte da rotina de backup da empresa.

5.5.5. São garantidos espaços em rede para cada finalidade específica: área de arquivos para o usuário, área de arquivos comuns aos departamentos, áreas especificas de cada departamento e áreas especiais com acessos controlados;

5.5.6. Os arquivos armazenados nos diretórios (pastas) da rede são de responsabilidade do usuário proprietário e do gestor da área, bem como a responsabilidade da manutenção (exclusão/organização) dos arquivos.

5.5.7. Não é permitido o uso e a instalação de software de qualquer natureza nos computadores da empresa sem o conhecimento e aprovação prévia do departamento de TI, seja essa realizada via internet, CD, DVD, Pendrive, ou outro meio.

5.5.8. Não é permitida a cópia ou execução de quaisquer aplicativos portáveis (softwares que não precisam ser instalados para funcionarem);

5.5.9. O uso de software de quaisquer tipos de jogos que precisam ou não de licença para sua execução, é terminantemente proibido nas dependências do TENIS CLUBE PAULISTA.

5.6. INSTALAÇÃO E UTILIZAÇÃO DOS SERVIDORES

5.6.1. Servidores devem estar obrigatoriamente instalados dentro de ambientes de Datacenter provisionados pela área de TI. Exceções devidamente autorizadas e motivadas por detalhes técnicos de instalação de equipamentos e softwares deverão ter backup garantido e suportado pela infraestrutura da área de TI.

5.6.2. É vetada qualquer instalação, configuração ou manutenção em servidores, exceto por administradores de rede e sistemas.

5.7. UTILIZAÇÃO DE EQUIPAMENTOS

5.7.1. Toda necessidade de mudança física do local de computadores, impressoras e outros equipamentos de TI, deverá ser previamente comunicada ao departamento de TI, por meio de chamado no sistema de Helpdesk, para que sejam tomadas as devidas providências.

5.7.2. É proibida a utilização de equipamentos particulares, inclusive microcomputadores portáteis, salvo autorizado pela gerência e área de TI, bem como utilizar celulares para captura de qualquer informação, principalmente dados protegidos pela LGPD.

5.7.3. É proibida a instalação ou configuração de qualquer equipamento que utilize a rede de computadores do TÊNIS CLUBE PAULISTA, sem a análise e autorização do departamento de TI;

5.7.4. É de responsabilidade do colaborador o manuseio correto dos equipamentos disponibilizados pelo TÊNIS CLUBE PAULISTA para cumprimento de suas atividades, bem como o cumprimento das recomendações constantes nos procedimentos operacionais;

5.7.5. É proibido qualquer procedimento de manutenção física ou logica, instalação, desinstalação, configuração ou modificação, troca ou mudança física, sem o conhecimento prévio e acompanhamento de um técnico da área de TI;

5.7.6. As instalações, configurações e dados armazenados nas estações de trabalho não possuem backup, portanto é de responsabilidade do usuário arquivar as informações relevantes no servidor de arquivos.

5.7.7. É proibido o acesso às estações de trabalho com o perfil de administrador por qualquer usuário de rede, exceto para usuários devidamente autorizados pela área de TI;

5.7.8. O uso de equipamentos de informática particulares que venham a se conectar as redes de comunicação da empresa deverão necessariamente:
serem previamente autorizados pela área de TI, possuir todos os softwares instalados na máquina, licenciados; receber instalação dos softwares de segurança utilizados no TÊNIS CLUBE PAULISTA (antivírus, VNC, etc.); receber configuração de perfil de usuário que impeça a instalação de novos softwares ou reconfiguração de sistema operacional do equipamento. Caso algum equipamento de usuário seja envolvido em atividade maliciosa ou danosa para a companhia, ele será recolhido e guardado pela área de TI, informando o DPO em caso da possibilidade de vazamento de dados pessoais, para permitir futuras investigações.

5.7.9. A utilização das impressoras é compartilhada, isto é, em caso de necessidade qualquer pessoa, independente de que área ela seja, pode fazer uso de qualquer impressora da empresa.

5.8. DISPOSITIVOS MÓVEIS

5.8.1. Quando se descreve dispositivo móvel, entende-se qualquer equipamento eletrônico com atribuições de mobilidade. Todos devem ser impreterivelmente homologados/aprovados pela área de TI. Ex.: notebooks, smartphones, tablets, pendrives, HD´s externos ou qualquer outro equipamento desta natureza.

5.8.2. É proibido o uso de dispositivos que permitem cópia de dados tais como: pendrive, HD externo, gravador de CD/DVD ou qualquer outro equipamento desta natureza. Exceções deverão ser devidamente acordadas e documentadas entre o gestor da área e o departamento de TI, que devem informar ao DPO.

5.8.3. Essa norma visa estabelecer critérios de manuseio, prevenção e responsabilidade sobre o uso de dispositivos móveis e deverá ser aplicada a todos os colaboradores que utilizem tais equipamentos.

5.8.4. O TÊNIS CLUBE PAULISTA reserva-se o direito de inspecionar os dispositivos móveis a qualquer tempo, caso seja necessário realizar uma manutenção ou auditoria de segurança.

5.8.5. O colaborador assume o compromisso de não utilizar, revelar ou divulgar a terceiros, de modo algum, direta ou indiretamente, em proveito próprio ou de terceiros, qualquer informação, confidencial ou não, que tenha ou venha a ter conhecimento em razão de suas funções no TENIS CLUBE PAULISTA, mesmo depois de terminado o vínculo contratual mantido com a empresa.

5.8.6. Não é garantido o backup de dados, instalações e configurações dos dispositivos móveis, salvo por ação do próprio usuário.

5.8.7. O suporte técnico aos dispositivos móveis de propriedade do TÊNIS CLUBE PAULISTA ou particulares, devidamente autorizados para uso nas instalações do TÊNIS CLUBE PAULISTA, deverá seguir o fluxo de suporte determinado pela área de TI através de chamado no sistema de Helpdesk; dispositivos particulares não autorizados para uso dentro das instalações da empresa, terão assistência negada por parte de TI.

5.8.8. É aconselhável que todo colaborador deva utilizar senhas de bloqueio automático para seu dispositivo móvel.

5.8.9. Não será permitido, em nenhuma hipótese, a alteração da configuração dos sistemas operacionais dos equipamentos, em especial as configurações referentes à segurança e à gravação de logs, sem a devida comunicação e a autorização da área responsável e sem a condução, auxílio ou presença de um técnico da área de TI.

5.8.10. O colaborador deverá responsabilizar-se em não manter ou utilizar quaisquer programas e/ou aplicativos que não tenham sido instalados ou autorizados pela área de TI.

5.8.11. A reprodução não autorizada dos softwares instalados nos dispositivos móveis fornecidos pelo TENIS CLUBE PAULISTA, constituirá uso indevido do equipamento e infração legal aos direitos autorais do fabricante.

5.8.12. É permitido o uso de rede banda larga de locais conhecidos pelo colaborador como a sua residência, hotéis, fornecedores e clientes;

5.8.13. É de responsabilidade do colaborador, no caso de furto ou roubo de um dispositivo móvel fornecido pelo TENIS CLUBE PAULISTA, notificar imediatamente a área de TI e seu respectivo gestor que deverão informar o DPO do ocorrido no momento que tiveram conhecimento. Também deverá procurar a ajuda das autoridades policiais, registrando assim que possível, um boletim de ocorrência (BO).

5.8.14. O colaborador deverá estar ciente de que o uso indevido do dispositivo móvel caracterizará a assunção de todos os riscos da sua má utilização, sendo ele o único responsável por quaisquer danos, diretos ou indiretos, presentes ou futuros, que venha a causar o TÊNIS CLUBE PAULISTA e/ou terceiros.

5.8.15. O colaborador que deseje utilizar equipamentos portáteis particulares ou adquirir acessórios e posteriormente conectá-los à rede do TÊNIS CLUBE PAULISTA, deverá submeter previamente tais equipamentos ao processo de autorização da área de TI.

6. RESPONSABILIDADES

6.1. GERAIS

6.1.1. Preservar a integridade e manter sigilo das informações de que fazem uso, bem como zelar e proteger os respectivos recursos de processamento de informações.

6.1.2. Cumprir esta política de segurança, estando sujeito às penalidades administrativas, cíveis e penais previstas pela legislação vigente.

6.1.3. Utilizar os sistemas de informações e os recursos a eles relacionados, somente para os fins ligados aos processos de negócios e interesses do TÊNIS CLUBE PAULISTA.

6.1.4. Cumprir as regras especificas de proteção estabelecidas aos ativos de informação e ativos de processamento.

6.1.5. Manter o caráter sigiloso da senha de acesso aos recursos e sistemas aplicativos.

6.1.6. Não compartilhar informações confidenciais e/ou privilegiadas com outras pessoas que não tenham a devida autorização de acesso.

6.1.7. Não compartilhar o usuário e senha ou outro meio de identificação, com outras pessoas.

6.1.8. Responder por todo e qualquer acesso aos recursos relacionados a ativos de informação e ativos de processamento, bem como pelos efeitos desses acessos efetivados através do seu código de identificação (User ID).

6.1.9. Respeitar a proibição de não usar, instalar, copiar ou armazenar programas de computador ou qualquer outro material relacionado à segurança da informação, incluindo-se material de terceiros, sejam eles em meio eletrônico ou convencional (papel), em violação da legislação de propriedade intelectual vigente.

6.1.10. Será de inteira responsabilidade de cada colaborador, todo prejuízo ou dano que vier a sofrer ou causar o TÊNIS CLUBE PAULISTA e/ou a terceiros, em decorrência da não observância às diretrizes e normas aqui referidas.

6.2. GESTORES

Além das regras gerais, todos os colaboradores que possuem cargo de liderança devem:

6.2.1. Gerenciar o cumprimento desta política de segurança, por parte de seus subordinados;

6.2.2. Impedir o acesso de colaboradores, terceiros e prestadores de serviços desligados aos ativos de informações, utilizando-se dos mecanismos de desligamento contemplados pelo respectivo processo de desligamento do colaborador;

6.2.3. Garantir que o pessoal sob sua supervisão compreenda e desempenhe a obrigação de proteger a informação conforme a política de segurança vigente;

6.2.4. Cabe ao gestor responsável por cada colaborador (funcionário ou terceiro) informar quando de um desligamento a área de RH, garantindo assim a devida notificação da área de TI para providências de bloqueio de acessos aos recursos

e sistemas informatizados e demais procedimentos que resguardem o TÊNIS CLUBE PAULISTA quanto a possibilidade de perda de informação;

6.2.5. O equipamento usado pelo usuário recém desligado deve ser entregue ao departamento de TI para que seja guardado ou disponibilizado a outro usuário conforme necessidade. Em hipótese alguma o equipamento deve permanecer no local ou ser realocado a outro usuário sem antes passar pelo departamento de TI;

6.2.6. Ter postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os colaboradores sob a sua gestão.

6.2.7. Informar qualquer procedimento que tenha risco de vazamento de dados pessoais ou inteirar de maneira imediata a possibilidade de vazamento de dados pessoais ao DPO.

6.3. GERÊNCIA DE TI

6.3.1. Estabelecer regras de proteção dos ativos de informação relacionados à PSI;

6.3.2. Direcionar quanto às medidas a serem tomadas no caso de violação das regras estabelecidas;

6.3.3. Revisar periodicamente, as regras de proteção estabelecidas;

6.3.4. Restringir e controlar o acesso e os privilégios de usuários com acesso remoto (externo);

6.3.5. Executar as regras de proteção estabelecidas por esta PSI;

6.3.6. Detectar, identificar, registrar e comunicar as violações ou tentativas de acesso não autorizadas;

6.3.7. Limitar o prazo/período de validade das contas de prestadores de serviço;

6.3.8. Fornecer acesso privilegiado somente aos colaboradores, terceiros e prestadores de serviço, que necessitem efetivamente dos privilégios, utilizando-se dos mecanismos de segurança e auditoria necessários;

6.3.9. Os administradores e operadores dos sistemas computacionais podem, pela característica de seus privilégios como usuários, acessar os arquivos e

dados de outros usuários. No entanto, isso só será permitido quando for necessário para a execução de atividades operacionais sob sua responsabilidade como, por exemplo, a manutenção de computadores, a realização de copias de segurança, auditorias ou testes no ambiente;

6.3.10. Configurar os equipamentos, ferramentas e sistemas concedidos aos colaboradores com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos por esta PSI;

6.3.11. Segregar as funções administrativas e operacionais a fim de restringir ao mínimo necessário os poderes de cada indivíduo e eliminar, ou ao menos reduzir, a existência de pessoas que possam excluir os logs e trilhas de auditoria das suas próprias ações;

6.3.12. Garantir segurança especial para os sistemas com acesso público (TS, serviço de correio, serviço WEB, VoIP, VPN), fazendo guarda de evidências que permitam a rastreabilidade para fins de auditoria ou investigação;

6.3.13. Gerar e manter as trilhas para auditoria sob demanda, com nível de detalhe suficiente para rastrear possíveis falhas e fraudes.

6.3.14. Administrar, proteger e testar as copias de segurança dos programas e dados relacionados aos processos críticos relevantes para o TENIS CLUBE PAULISTA;

6.3.15. Implantar controles que gerem registros auditáveis para retirada e transporte de mídias das informações custodiadas pela TI, nos ambientes totalmente controlados por ela;

6.3.16. Quando ocorrer movimentação interna dos ativos de TI, garantir que as informações de um usuário não serão removidas de forma irrecuperável antes de disponibilizar o ativo para outro usuário;

6.3.17. Proteger continuamente todos os ativos de informação da empresa contra código malicioso (vírus), e garantir que todos os novos ativos só entrem para o ambiente de produção, após estarem livres de código malicioso e/ou indesejado;

6.3.18. Garantir que não sejam introduzidas vulnerabilidades ou fragilidades no ambiente de produção da empresa em processos de mudança, sendo ideal a auditoria de código e a proteção contratual para controle e responsabilização no caso de uso de terceiros;

6.3.19. Definir as regras formais para a instalação de software e hardware em ambiente de produção corporativo, exigindo o seu cumprimento dentro da empresa;

6.3.20. Realizar auditorias periódicas de configurações técnicas e análise de riscos;

6.3.21. Garantir, da forma mais rápida possível, mediante solicitação formal do demandante, o bloqueio de acesso de usuário por motivo de desligamento da empresa, incidente, investigação ou outra situação que exija medida restritiva para fins de salvaguardar os ativos da empresa.

6.3.22. Informar qualquer procedimento que tenha risco de vazamento de dados pessoais ou inteirar de maneira imediata a possibilidade de vazamento de dados pessoais ao DPO.

6.4 DPO – DATA PROTECTION OFFICER

6.4.1. A principais funções do serviço de DPO oferecido são:

- Conhecer todo o procedimento de implementação ou adequação da Lei Geral de Proteção de Dados utilizada desde no início;
- Responsável pelo Gerenciamento e Organização da Proteção de Dados implantada na empresa;

- Entender a responsabilidade dos atores da lei – Controlador, Operador, Titular e Autoridade Nacional de Proteção de Dados (ANPD) – para tomar as providencias necessárias em caso de vazamento de dados;
- Implementação do Controlador e do Operador no tratamento de dados;
- Conhecer e entender sobre Relatório de Impacto;

• Conhecer os procedimentos adotados quando houver uma violação de dados, ou vazamento de dados;

• Conhecer e manter atualizado a Política de Proteção de Dados, Objetivo das Políticas de Proteção de Dados/ Privacidade em uma Organização;

• Compreender os conceitos de proteção de dados desde a concepção (by design) e por padrão (by defaul).

7. PROCEDIMENTOS

7.1. ACESSO A SISTEMAS E SERVIÇOS DE TI

7.1.1 Os acessos a todos os recursos de TI os quais os usuários devem ter acesso, deve ser informado através do preenchimento do formulário Ficha de Usuário - ZZZZZ e anexado a um chamado encaminhado por e-mail solicitando seu cadastro;

8. ANEXOS

Não se aplica.

9. CONSIDERAÇÕES FINAIS

Esta Política foi aprovada pela Diretoria Executiva do TÊNIS CLUBE PAULISTA em 01/02/2025 e entrou em vigor logo após a data da aprovação, sendo sua divulgação disponibilizada a todos os colaboradores do TÊNIS CLUBE PAULISTA e demais interessados pelo canal de comunicação interno da empresa ou pelo site.

www.tenisclubepaulista.com.br/