	RESOLUÇÃO NORMATIVA (RN)	RN-024/00
EMITENTE **Diretoria de Informática**		**APROVADA PELA DIRETORIA** RN – 024/00 – DE 14/1/2020
ASSUNTO **Política de Segurança da Informação**		ABRANGÊNCIA **GERAL**

1. OBJETIVOS

1.1 Estabelecer diretrizes e procedimentos que permitam aos colaboradores do Club Athletico Paulistano (CAP) seguirem padrões de comportamento relacionados à segurança da informação adequada às necessidades de negócio e de proteção legal do CAP e do indivíduo.

1.2 Definir normas e procedimentos específicos de segurança da informação, bem como implementar controles e processos para seu atendimento.

2. ABRANGÊNCIA

2.1 Esta política aplica-se a todos os funcionários, estagiários, prestadores de serviços, enfim, todos os colaboradores e associados, ou seja, todos os usuários que venham a ter acesso aos ativos de TI (Tecnologia da Informação) do CAP.

3. CONCEITOS

3.1 A segurança da informação é aqui caracterizada pela preservação dos seguintes conceitos:

3.1.1 Integridade: garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais.

3.1.2 Confidencialidade: garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.

3.1.3 Disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário, estabelecendo um cronograma de planejamento de implementação das medidas a serem executadas.

3.2 Das condições de uso

3.2.1 As condições de uso definem os padrões e as recomendações de segurança que os usuários devem cumprir para obter acesso aos ativos de TI do Club Athletico Paulistano.

3.2.2 Os ativos de TI são de propriedade do CAP e de uso exclusivo para execução dos trabalhos.

4. RESPONSABILIDADES

4.1 É responsabilidade de todo usuário

4.1.1 Utilizar os ativos de TI de forma responsável, profissional, ética, sustentável e legal.

4.1.2 Respeitar a integridade, a disponibilidade, a privacidade e a confidencialidade das informações do CAP e de seus usuários.

4.1.3 Respeitar os direitos e as permissões de uso dos ativos de TI concedidos pelo CAP.

4.1.4 Respeitar e seguir o "código de práticas" deste documento.

4.1.5 Seguir as normas e os procedimentos de atendimento aos usuários dos ativos de TI (Sustentação), informando corretamente o problema e o nível de prioridade.

4.2 Restrições de uso

4.2.1 Permissão de acesso aos ativos de TI somente após a assinatura do *"Termo de Confidencialidade e Responsabilidade na Utilização de Recursos Computacionais e da Informação"* junto ao Departamento de Recursos Humanos (RH).

4.2.2 Os ativos de TI não podem ser utilizados para difusão ou armazenamento de propaganda pessoal ou comercial, aliciamentos, programas destrutivos (vírus e spam), material político ou qualquer outro uso inadequado.

4.2.3 É expressamente proibido o uso da infraestrutura computacional por qualquer indivíduo que não mantenha contrato direto ou indireto com o CAP.

4.2.4 O uso da infraestrutura computacional é um recurso que pode ser revogado ou restringido a qualquer momento, caso ocorra algum incidente relatado.

4.3 Restrições de conteúdo

4.3.1 É expressamente proibido o armazenamento ou transmissão, sob qualquer forma ou meio de comunicação, de conteúdo inapropriado que promova, incite ou instrua ações e atitudes, tais como: crime, roubo, violência, terrorismo, difamação, calúnia, preconceito de qualquer tipo ou classe, drogas e pornografia.

4.4 Uso de hardware

4.4.1 É proibido aos usuários:

4.4.1.1 Disponibilizar o acesso a pessoas não autorizadas.

4.4.1.2 Instalar ou alterar as configurações do hardware sem autorização formal do Departamento de Tecnologia da Informação.

4.4.1.3 Instalar servidores, computadores, periféricos e acessórios na infraestrutura computacional, sem prévia autorização formal do Departamento de Tecnologia da Informação.

4.4.1.4 Promover qualquer manutenção ou tentativa de manutenção dos ativos de TI.

4.5 Uso de software

4.5.1 É proibido aos usuários:

4.5.1.1 Copiar softwares do CAP.

4.5.1.2 Disponibilizar cópias de softwares para terceiros ou fornecedores do CAP.

4.5.1.3 Instalar qualquer tipo de softwares.

4.5.1.4 Alterar configurações de softwares instalados.

4.5.1.5 Utilizar técnicas de engenharia reversa ou decompilar softwares de propriedade do CAP.

4.5.1.6 Utilizar licenças de softwares que infrinjam quaisquer patentes ou direitos autorais.

4.6 Suporte aos usuários e manutenção dos ativos de TI homologado pelo Club Athletico Paulistano.

4.6.1 O suporte aos usuários dos ativos homologados pelo CAP é restrito à equipe técnica da área de TI.

4.6.2 A manutenção dos ativos de TI homologados pelo CAP é restrita às empresas contratadas por meio da área de TI e somente elas poderão promover qualquer intervenção técnica, sob pena de perda de garantia dos ativos.

5. CONTINGÊNCIA

5.1 É reservado ao CAP, através da Equipe de Sustentação de TI, o direito à adoção de medidas emergenciais para preservar a segurança dos seus ativos, efetuando suspensão, bloqueio e alteração de contas e de senhas além de cancelamento de processo em andamento, dentre outros, de quaisquer usuários.

5.2 Alterações da política de segurança

5.2.1 Esta política será revisada e/ou atualizada anualmente pela Diretoria de Tecnologia da Informação, de acordo com as necessidades do CAP. Todos os usuários serão informados quando ocorrerem tais revisões/atualizações.

5.3 Estrutura Normativa

5.3.1 A estrutura normativa da Segurança da Informação do CAP é composta por um conjunto de documentos denominados “Políticas e Procedimentos de Tecnologia da Informação” (PPTI), que definem a estrutura, as diretrizes e os papéis referentes à segurança da informação, instrumentando as regras dispostas, permitindo a direta aplicação nas atividades do CAP.

5.3.2 Faz parte do escopo das PPTI indicar quais são as práticas mais adequadas para a utilização dos ativos de TI, observando aspectos peculiares a cada tipo de aplicação ou serviço.

5.4 Hardware

5.4.1 Os ativos de hardware de TI devem ter seu uso racional, observando os limites de utilização estabelecidos pelo CAP.

5.4.2 É dever de todos os usuários protegerem os ativos de TI contra qualquer tipo de danos e perdas.

5.4.3 Somente o Departamento de Tecnologia da Informação poderá efetuar e/ou autorizar qualquer tipo de alteração e reparo interno ou externo nos ativos.

5.4.4 Os usuários dos ativos de TI somente estão autorizados a utilizar os hardwares homologados pelo CAP.

5.4.5 Poderão ter acesso à rede corporativa, mediante autorização do Departamento de TI, todos os ativos não pertencentes ao CAP, tais como: computadores, celulares, pen drives, discos rígidos externos, câmeras digitais, etc.

5.5 Das movimentações dos ativos de TI

5.5.1 Na necessidade de transportar um ativo de TI para realização de trabalhos externos, é necessária autorização do gerente da área responsável.

5.5.2 As movimentações dos equipamentos de TI devem ser efetuadas por meio de chamados e devem ser realizadas pela Equipe de Sustentação do Departamento de TI.

5.5.3 Movimentações de equipamentos de TI para manutenção devem ser feitas apenas pelo Departamento de TI.

5.6 Software

5.6.1 Os ativos de software de TI devem ter seu uso racional, observando os limites de utilização estabelecidos pelo CAP.

5.6.2 É dever de todos os usuários protegerem os ativos de TI contra qualquer tipo de danos e perdas.

5.6.3 Os usuários dos ativos de TI somente estão autorizados a utilizar os softwares homologados pelo CAP.

5.6.4 Os softwares gratuitos poderão ser utilizados apenas quando justificados, autorizados e instalados pela Equipe de Sustentação de TI.

5.6.5 É expressamente proibido instalar qualquer tipo de software, principalmente os que infrinjam quaisquer patentes ou direitos autorais e utilização de técnicas de engenharia reversa, objetivando decompilar os softwares de propriedade da entidade.

6. VÍRUS

6.1 Os vírus podem causar danos em diversos níveis chegando a afetar a integridade de arquivos de dados, causando prejuízos imensuráveis e, em alguns casos, irrecuperáveis. Portanto, cada usuário é responsável por tomar precauções para evitar a contaminação dos computadores.

6.2 O CAP fornece as ferramentas necessárias para a detecção e a eliminação de vírus de computadores e programas do tipo: trojan, blaster, cavalos de tróia, spams, etc.

6.3 Os usuários dos ativos de TI comprometem-se a:

6.3.1 Não executar programas ou arquivos de fontes desconhecidas provenientes da internet e sempre verificar os arquivos recebidos quanto à existência de vírus (via internet, redes de terceiros, disquetes, CDs, DVDs, cartão de memória, unidades de disco removível) por meio das ferramentas fornecidas pelo CAP para esta finalidade.

6.3.2 Comunicar ao Departamento de TI, quando percebido, qualquer incidente de vírus, pois caberá exclusivamente a Equipe de Sustentação informar os procedimentos a serem adotados sobre vírus.

7. BANCO DE DADOS

7.1 As informações contidas nos sistemas de banco de dados do CAP são de seu uso exclusivo.

7.2 O banco de dados com informações de associados possui política de privacidade específica de utilização.

7.3 É vedada a cópia ou uso não autorizado destes dados para outros fins, que não sejam de interesse do CAP.

7.4 Os usuários deverão zelar pela integridade, disponibilidade e confidencialidade destas informações.

8. CORREIO ELETRÔNICO

8.1 O sistema de correio eletrônico deverá ser utilizado somente para atividades relacionadas à instituição e que contribuam positivamente para o CAP.

8.2 É expressamente proibido:

8.2.1 Enviar ou ser conivente com conteúdo não aderente a esta política de segurança.

8.2.2 Enviar mensagens para listas de fornecedores e parceiros que não sejam de interesse da entidade, sem a devida autorização da área responsável.

8.2.3 Enviar mensagens que configurem phishing para usuários internos e externos.

8.2.4 Enviar mensagens com a identificação do remetente alterada ou falsificada.

8.2.5 Enviar mensagens com o conteúdo alterado ou falsificado.

8.2.6 Invadir a privacidade de usuários pelo acesso não autorizado à sua caixa postal.

8.2.7 Enviar informações confidenciais do CAP para redes públicas (internet), sem autorização.

9. REDE DE COMPUTADORES

9.1 A rede de computadores da entidade deve ser utilizada de forma proficiente e produtiva, mantendo sua integridade, disponibilidade e confidencialidade das informações e de seu conhecimento.

9.2 É expressamente proibido o uso, sem autorização, de softwares não aderentes à política de segurança do CAP.

9.3 Seja localmente em seu computador ou por meio da rede, os usuários não podem alterar copiar e/ou excluir arquivos pertencentes a outro usuário sem primeiro obter sua permissão.

9.4 A rede não deve ser utilizada para transmitir ou armazenar informações que não sejam do interesse ou não contribuam com os objetivos do CAP.

9.5 Ao se ausentar ou sair, o usuário deverá desconectar seu login aberto ou bloquear sua estação de trabalho, para que não haja utilização indevida dos ativos de TI.

9.6 Todo usuário deve fazer uso racional dos recursos, observando os limites de utilização estabelecidos pela política de segurança da entidade.

10. INTERNET

10.1 A internet, por sua diversidade de plataformas e pela quantidade de computadores e usuários, propicia o surgimento e a disseminação de vírus em variados formatos, de conteúdo ilegal e de outros incidentes de segurança.

10.2 Devem ser adotadas as seguintes práticas:

10.2.1 Como todo o tráfego de utilização da internet será monitorado, mediante solicitação, relatórios de utilização poderão ser emitidos e divulgados de acordo com os critérios estabelecidos pela equipe de TI.

10.2.2 Todo o conteúdo recebido ou enviado através da internet será automaticamente submetido a verificações de segurança para eliminação de vírus e tentativas de invasão da rede corporativa.

10.2.3 O CAP não se responsabilizará por problemas ocasionados em virtude do fornecimento de informações pessoais dos seus usuários na internet, tais como: números de cartão de crédito ou contas-correntes bancárias e senhas para acesso a sistemas de internet banking.

10.2.4 Novos recursos na internet, além do acesso à web e ao correio eletrônico, deverão ser liberados somente mediante prévia análise de riscos de segurança e comprovação da necessidade e/ou benefícios do serviço para o CAP.

11. SUPORTE AOS USUÁRIOS DOS ATIVOS DE TI

11.1 O suporte aos ativos de TI é realizado de acordo com os horários de atendimentos estabelecidos pelo CAP, por meio de abertura de chamado técnico.

11.2 É de responsabilidade do Departamento de TI certificar-se de que o atendimento e a solução proposta seguem os padrões e o tempo estabelecidos.

11.3 Sistemas corporativos:

11.3.1 Os usuários não podem instalar ou utilizar qualquer tipo de sistema ou aplicativos para desenvolvimento de bases de informação, paralelas aos sistemas corporativos adotados e homologados pelo CAP.

11.3.2 São de responsabilidade do usuário todas as informações inseridas por ele nos sistemas corporativos do CAP**.**

11.3.3 Os usuários devem comprometer-se a informar quaisquer problemas encontrados nos sistemas do CAP, podendo facultativamente dar sugestões para a sua melhoria, por meio da Equipe de Sustentação de TI.

11.4 Homologação

11.4.1 Qualquer solicitação do usuário atendida por meio de atualização parcial ou total de sistema, será apenas implantada em produção após a aprovação do usuário responsável pela solicitação.

11.5 Formalização de criação de usuários e perfis de ativos de TI

11.5.1 Termo de compromisso para usuários de ativos de TI:

11.5.1.1 Todos os colaboradores deverão previamente assinar o *"Termo de Confidencialidade e Responsabilidade na Utilização de Recursos Computacionais e da Informação"* no Departamento de RH, que trata do de acordo aos padrões e às recomendações estabelecidas nas contratações do CAP e entregas através do Departamento de Recursos Humanos.

11.5.2 Criação de usuários para os sistemas legados do CAP:

11.5.2.1 A criação de usuário deve ser solicitada mediante chamado e desde que este usuário esteja devidamente cadastrado no Sistema de Administração de Recursos ou, se associado, no sistema de Gestão de Associados do Clube.

11.5.2.2 Os direitos de acesso devem ser solicitados de acordo com as necessidades do Departamento devidamente cadastrado em um GRUPO para a execução das suas atividades

11.5.2.3 Quando houver mudança nas atribuições de um Usuário da Rede/Sistemas ou quando ocorrer seu remanejamento para outro setor, os direitos de acesso deverão ser readequados, por solicitação dos superiores imediatos.

11.6 Rescisão de contrato de trabalho

11.6.1 O término e a rescisão dos contratos de trabalho, de prestação de serviços em geral ou quaisquer outros tipos de Convênios, Acordos e Termos com o CAP implicarão extinção imediata de todos os direitos de uso e acesso aos ativos de TI que possuía o indivíduo ou empresa.

11.6.2 Cabe ao Departamento de Recursos Humanos informar à Equipe de Tecnologia da Informação sobre as rescisões de colaboradores em geral, garantindo a segurança contra acessos indevidos, após o término do período estabelecido para utilização dos ativos de TI.

11.6.3 A Equipe de Tecnologia da Informação poderá providenciar backup (cópia) das informações do usuário que estiver em processo de rescisão contratual, quando solicitado pelo gestor da área pertinente.

11.7 Revisão de acesso

11.7.1 Os sistemas adquiridos devem emitir relatórios com usuários ativos e seus respectivos perfis, para que o gestor da área de Negócio revise.

11.7.2 As revisões devem acontecer, no mínimo, 2 (duas) vezes por ano.

11.7.3 Eventuais inconsistências devem ser apontadas pelo gestor para que sejam corrigidas.

12. SENHAS

12.1 As seguintes práticas devem ser observadas:

12.1.1 Após efetuar seu primeiro acesso à rede corporativa por meio de uma senha fornecida pela equipe técnica da área de TI, o usuário receberá um aviso automático solicitando a mudança para uma nova senha.

12.2 Senhas devem ser memorizadas, nunca escritas e/ou registradas em papel ou digitalmente.

12.3 Senhas são individuais e nunca poderão ser compartilhadas com outros usuários.

12.4 Senhas devem ser trocadas a cada três 3 (três) meses, ou imediatamente, se comprometidas.

12.5 O usuário deve adotar como regra de formação de senhas:

12.5.1 Escolher senhas com 8 (oito) ou mais caracteres, compostos sempre por letras e números em conjunto.

12.5.2 Mesmo estando os sistemas configurados para minimizar a ocorrência de senhas vulneráveis, nunca deverão ser escolhidas senhas óbvias baseadas em: datas de aniversário da pessoa ou parentes, nomes abreviados, nomes próprios, apelidos, nomes de parentes, números de telefone, dentre outros.

12.5.3 Nunca utilize como senha o login de acesso à rede ou ao sistema.

12.5.4 Nunca escolha senhas baseadas em palavras contidas em dicionários. Grande parte dos incidentes de segurança ocorre por meio de métodos de exploração de senhas por força bruta utilizando, por exemplo, todas as palavras de um dicionário armazenadas em um banco de dados como possíveis senhas.

12.5.5 Use símbolos do tipo "%", "-" ou "$" para formar a senha.

12.6 A TI deverá evitar ou, se adquirir, justificar junto a área de Negócio, sistemas que não permitem senhas seguras.

12.7 A TI executará procedimentos periódicos de verificação de vulnerabilidade de senhas para identificar se a escolha foi inadequada e solicitar a respectiva alteração, se for o caso.

13. DO MONITORAMENTO DE TRÁFEGO E SEGURANÇA

13.1 Os ativos de TI e quaisquer informações e conteúdos neles armazenados pertencem ao CAP e, sendo assim, serão submetidos a processos de monitoramento de tráfego e segurança, garantindo estabilidade, integridade, disponibilidade e confidencialidade do ambiente.

13.2 O CAP não necessitará de qualquer tipo de aviso ou autorização judicial para executar tais ações.

14. DA AUDITORIA DE CONTEÚDO

14.1 Os ativos de TI e quaisquer informações e conteúdos neles armazenados pertencem ao CAP e, sendo assim, poderão ser submetidos a processos de auditoria, caso ocorram incidentes de segurança.

14.1.1 Tal processo só poderá ser autorizado pela Diretoria Executiva de Tecnologia da Informação.

15. DA COMUNICAÇÃO DOS INCIDENTES E MEDIDAS DISCIPLINARES

15.1 Comunicação

15.1.1 Todos os incidentes de segurança deverão ser relatados à Equipe de TI imediatamente.

15.1.2 A conivência ou omissão por parte dos usuários perante os incidentes de segurança é considerada grave incidente.

15.2 Medidas Disciplinares

15.2.1 Nos casos de transgressões desta política de segurança, os usuários estarão sujeitos à aplicação de medidas disciplinares, que poderão levar à demissão ou à rescisão de contrato e também às penalidades previstas nas legislações cível, trabalhista e penal.

Aprovação

_____

Paulo Cesar Mario Movizzo
Presidente da Diretoria

Resolução Normativa elaborada pela Comissão de Normatização

Maria Christina Horta de Araujo e Rocha Ferreira (Presidente)
Beatriz Maria de Castro Oliveira
Geraldo Santamaria Filho
Luiz Alberto Moraes Chaib
Maria José Nascimento Corrêa
Mario Francisco Teixeira da Silva