	RESOLUÇÃO NORMATIVA (RN)	**RN-024/01**
EMITENTE **Diretoria de Tecnologia da Informação**		**APROVADA PELA DIRETORIA** RN-024/00 – DE 14/01/2020 RN 024/01 – DE 26/05/2025
ASSUNTO **Plano de Gestão de Segurança da Informação**		ABRANGÊNCIA **GERAL**

1. OBJETIVOS

1.1 Este plano tem como objetivo atender a Política de Segurança da Informação que visa a criar um ambiente seguro no qual o CAP possa operar e proteger seus ativos de informação.

1.2 E, garantir que as informações críticas estejam disponíveis, íntegras e confidenciais, contribuindo para a confiabilidade, conformidade e eficiência geral das operações do CAP.

2. SEGURANÇA DA INFORMAÇÃO

2.1 A gestão de segurança da informação é um conjunto de processos, metodologias e procedimentos.

2.2 Foram desenvolvidos e implementados para garantir a confidencialidade, integridade e disponibilidade das informações, atuando contra acessos não autorizados, mau uso, divulgações indevidas, cópias não autorizadas, destruição ou alterações.

2.3 Ela envolve a implementação de procedimentos, práticas e tecnologias com o propósito de garantir que os dados e informações críticas do CAP sejam protegidos de maneira eficaz, reduzindo riscos e garantindo a integridade e a confiabilidade desses ativos.

3. RESPONSABILIDADES E ESTRUTURA ORGANIZACIONAL DA SEGURANÇA DA INFORMAÇÃO

3.1 Diretoria

3.1.1 O CAP reafirma seu compromisso com a segurança da informação, bem como com o cumprimento das leis e regulamentações aplicáveis ao negócio.

3.1.2 Para esse fim, foi criado o Portal da Privacidade, acessível através do endereço eletrônico https://www.paulistano.org.br/portal-de-privacidade/. Nesse portal, todos podem obter informações essenciais sobre a Lei Geral de Proteção de Dados, conhecer seus direitos como titulares de dados, e entender em detalhes como o CAP trata e protege suas informações pessoais.

3.1.3 Além disso, elaborou Políticas de Privacidade, Segurança da Informação e Procedimentos de Tecnologia da Informação que definem a estrutura, as diretrizes e os papéis referentes à segurança da informação.

3.2 Gestor de Tecnologia da Informação

3.2.1 O Gestor de TI desempenha um papel crucial na administração e segurança dos sistemas de informação de uma organização.

3.2.2 Suas responsabilidades abrangem a definição, implementação e manutenção de procedimentos tecnológicos que garantem a integridade, confidencialidade e disponibilidade das informações.

3.2.3 Este papel envolve várias etapas e áreas de atuação, sendo as principais: planejamento e concepção de soluções tecnológicas; implementação de sistemas de segurança; resposta a incidentes; gestão e manutenção; controle e auditoria, treinamento e conscientização e alinhamento estratégico.

3.2.4 Ao integrar todos esses aspectos, o Gestor de TI não apenas protege os ativos digitais do CAP, mas também contribui para a eficiência operacional e alcance dos objetivos estratégicos.

3.3 Lideranças

3.3.1 A liderança desempenha um papel vital na segurança da informação.

3.3.2 Suas responsabilidades vão além da simples implementação de políticas e procedimentos, abrangendo uma visão estratégica e uma cultura organizacional que prioriza a segurança da informação em todos os níveis.

3.3.3 Este papel envolve várias etapas e áreas de atuação, sendo as principais: cultura de segurança; alocação de recursos; governança e conformidade; gestão de riscos; treinamento e conscientização; monitoramento e revisão; engajamento e comunicação e liderar pelo exemplo.

3.4 Encarregado pelo Tratamento de Dados Pessoais

3.4.1 Dentre outras atribuições, nos termos do art. 41, §2º, da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados - LGPD), é responsável por conduzir o diagnóstico de privacidade, bem como orientar, no que couber, os gestores proprietários dos ativos de informação, responsáveis pelo planejamento, implementação e melhoria contínua dos controles de privacidade em ativos de informação que realizem o tratamento de dados pessoais e dados pessoais sensíveis.

3.5 Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação

3.5.1 Composta por profissionais da área de Tecnologia da Informação com capacidade técnica compatível com essas atribuições. A atuação da equipe será regida por normativos, padrões e procedimentos técnicos definidos no documento PPTI-07 “Políticas e Procedimentos de Tecnologia da Informação – Gestão de Incidentes”.

4. SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO

4.1 O Sistema de Gestão de Segurança da Informação é composto por um conjunto de documentos denominados Políticas e Procedimentos de Tecnologia da Informação – PPTI.

4.2 Eles definem a estrutura, as diretrizes e os papéis referentes a segurança da informação, e instrumentam as regras dispostas, permitindo a direta aplicação nas atividades do CAP. Tais procedimentos garantem a privacidade e a segurança da informação, como também a conformidade com a legislação pertinente.

4.3 O Sistema de Gestão de Segurança da Informação do CAP inclui uma abordagem para proteger a informação de acordo com os princípios e atributos de confidencialidade, disponibilidade, integridade, responsabilidade, autenticidade e criticidade.

4.4 Ele envolve vários processos organizacionais, entre eles: classificação da informação; gestão de resposta a incidentes cibernéticos; controle de acesso à informação; gestão de ativos de tecnologia da informação; conscientização; educação e treinamento em segurança da informação; dentre outros processos.

4.5 **Processos e Programa de Gestão de Segurança da Informação**

4.5.1 Na gestão de privacidade e segurança da informação do CAP, vários processos e programa que compõem a segurança da informação estão interrelacionados de forma a possibilitar a gestão da segurança da informação integrada aos demais processos organizacionais.

4.5.2 Abaixo, relacionamos alguns dos processos relativos à privacidade e segurança da informação.

4.5.2.1 Gestão de dados.

4.5.2.2 Conscientização, educação e treinamento.

4.5.2.3 Gestão de Auditoria e conformidades.

4.5.2.4 Gestão de vulnerabilidade.

4.5.2.5 Segurança física do ambiente.

4.5.2.6 Gestão de incidente de segurança da informação.

4.5.2.7 Gestão de ativos.

4.5.2.8 Gestão de infraestrutura de rede.

4.5.2.9 Gestão de controle de acesso.

4.5.2.10 Gestão de *software.*

4.5.2.11 Gestão de fornecedores e terceiros.

4.5.2.12 Gestão de recuperação de dados.

4.5.2.13 Gestão de riscos de segurança da informação.

4.5.3 Para cada processo e programa, existem medidas de controles a serem implementadas para assegurar a disponibilidade, integridade, confidencialidade e a autenticidade da informação.

4.6 **Controle de Privacidade e Segurança da Informação**

4.6.1 A gestão de segurança da informação envolve controles de privacidade e segurança da informação. Estes controles envolvem rotinas para gestão de ativos da informação, classificação da informação, riscos de segurança da informação, gestão contínua de vulnerabilidades, proteção e recuperação de dados e educação de usuários.

4.6.2 Abaixo, apresentaremos os controles que compõem a segurança da informação no CAP.

4.6.2.1 Teste de invasão.

4.6.2.2 Gestão de incidentes.

4.6.2.3 Segurança de aplicações.

4.6.2.4 Gestão de provedor de serviços.

4.6.2.5 Conscientização e treinamento de competências sobre segurança.

4.6.2.6 Monitoramento e defesa de rede.

4.6.2.7 Gestão de infraestrutura de rede.

4.6.2.8 Recuperação de dados.

4.6.2.9 Defesa contra *malware*.

4.6.2.10 Proteção de *e-mail* e navegador *web*.

4.6.2.11 Gestão de registro de auditoria.

4.6.2.12 Gestão contínua de vulnerabilidades.

4.6.2.13 Gestão de controle de acesso.

4.6.2.14 Gestão de contas.

4.6.2.15 Configuração segura de ativos institucionais e *software*.

4.6.2.16 Proteção de dados.

4.6.2.17 Inventário e controle de ativos de *software*.

4.6.2.18 Inventário e controle de ativos institucionais.

4.6.3 **Classificação e Tratamento da Informação**

4.6.3.1 O proprietário da informação é responsável por classificá-la adequadamente, aplicando o nível de proteção proporcional à sua importância e por rotulá-la com o nível de segurança adequado.

4.6.3.2 As informações só podem ser divulgadas externamente quando autorizadas pelo proprietário, salvo quando envolver ordens judiciais.

4.6.3.3 As informações, em especial os dados pessoais (incluindo as sensíveis), devem ser utilizadas unicamente para a finalidade para a qual foram coletadas, conforme diretrizes da LGPD.

4.6.3.4 As informações do CAP, ou de sua responsabilidade, devem ser classificadas de acordo com seu valor para o negócio e sensibilidade, utilizando os níveis de segurança para classificação dos dados.

4.6.3.5 O proprietário da informação é responsável por assegurar que as informações estejam controladas, de forma a garantir que apenas as pessoas autorizadas possam acessá-las.

4.6.3.6 Os dados lógicos confidenciais têm restrições que só permitem o acesso por pessoas autorizadas.

4.6.3.7 As informações analógicas confidenciais têm controle de acesso para as salas e, quando armazenados externamente, são selecionadas empresas que garantam a segurança da informação.

4.6.3.8 Todas as categorias de informação têm processos de integridade e disponibilidade.

4.6.4 **Gestão de Acessos**

4.6.4.1 A gestão dos direitos, alteração e revogação de acessos aos ativos é cadastrada e controlada. As regras estão documentadas no PPTI 01- Gestão de Acesso Usuários.

4.6.5 **Segurança Física e do Ambiente**

4.6.5.1 Foram definidos os controles para prevenir o acesso físico nas dependências do CAP e no Data Center, de forma a manter os recursos essenciais para operação dos ativos e evitar danos e interferências nos recursos de processamento das informações.

4.6.5.2 A infraestrutura necessária para operação segura dos ativos é gerenciada e os recursos críticos são controlados e submetidos à manutenções regulares para assegurar o seu funcionamento.

4.6.5.3 O acesso ao Data Center é regulamentado conforme o PPTI 03 – Acesso ao Data Center.

4.6.6 **Segurança das Operações**

4.6.6.1 Os empregados são orientados quanto a importância dos cuidados com as informações em lugares públicos e fora do ambiente de controle.

4.6.6.2 Para que seja permitido a troca de informações entre o CAP e partes externas, são estabelecidos acordos de confidencialidade.

4.6.6.3 O uso de sistemas de comunicações eletrônicas, e todas as mensagens geradas ou transmitidas através do mencionado sistema, são consideradas propriedades do CAP.

4.6.6.4 O acesso à caixa de correio eletrônico se dará através de *software* específico, cuja configuração será feita pelo Departamento de Tecnologia da Informação.

4.6.6.5 O conteúdo e o uso de sistemas de comunicações eletrônicas são monitorados para apoiar as atividades de manutenção, segurança, auditoria e outras investigações.

4.6.6.6 Os usuários devem utilizar as comunicações eletrônicas tendo em mente o fato de que o CAP se reserva no direito de examinar o conteúdo delas.

4.6.6.7 É responsabilidade do usuário, ao receber mensagens de origem desconhecida ou que contenham arquivos anexos duvidosos, não abrir ou executar tais anexos e encaminhar tais mensagens imediatamente ao Departamento de Tecnologia da Informação.

4.6.7 **Proteção contra *Malwares***

4.6.7.1 As estações de trabalho do CAP possuem solução de antivírus instalada e gerenciada através de uma plataforma que integra todos os *logs* de atividades suspeitas e de ameaças de *softwares* maliciosos, impedindo a ação de *malwares* e fazendo as verificações em arquivos e/ou dispositivos de mídia.

4.6.7.2 A plataforma de gerenciamento distribui atualizações sempre que necessário. A partir dessa plataforma é possível visualizar todas as máquinas e qualquer ação suspeita.

4.6.7.3 Todos os novos colaboradores recebem no *Onboarding* a orientação sobre os riscos referentes à vírus e as melhores práticas de comportamento seguro na rede, devendo tomar precauções para evitar a contaminação dos computadores.

4.6.8 **Cópias de Segurança**

4.6.8.1 O CAP conta com um sistema de *backup* totalmente automatizado, realizando *backups* da infraestrutura de máquinas e arquivos e da informação relevante para operação dos negócios.

4.6.9 **Instalação Padrão**

4.6.9.1 A instalação inicial dos sistemas de uso interno e antivírus é orientada através do uso de *check list* de preparação do equipamento. Um conjunto padrão de instalação de *softwares* é preparado e mantido em local seguro.

4.6.9.2 Estas cópias padrão são usadas para a recuperação de infecções de vírus, falhas do disco rígido e outros problemas do equipamento.

4.6.9.3 O uso ou instalação de *software* ou *hardware* só é permitido quando devidamente homologado e licenciado.

4.6.9.4 Todos os colaboradores são monitorados e, em caso de identificação de *software* não licenciado, a equipe da TI notifica o usuário e depois verifica se foi desinstalado, ou se foi adquirido.

4.6.9.5 *Softwares* são utilizados para a realização de inventário de instalações, com o intuito de verificar e identificar possíveis instalações não permitidas.

4.6.10 **Auditorias de Sistema da Informação**

4.6.10.1 As auditorias de sistema são realizadas extraordinariamente e o registro é armazenado no repositório da TI.

4.6.10.2 Eventuais não conformidades identificadas serão registradas e tratadas. Além das auditorias extraordinárias, é realizada a verificação e registrado o monitoramento de forma constante através dos alertas de segurança sistêmicos.

4.6.10.3 Os resultados dessas auditorias são submetidos ao Gestor de TI, que avalia e informa ao Diretor.

4.6.11 **Segurança nas Comunicações**

4.6.11.1 A rede corporativa do CAP possui implementações de segurança que impedem que pessoas externas à organização acessem seus recursos.

4.6.11.2 Para acessar a rede é necessário autenticação através de *login* e senha.

4.6.11.3 A rede é monitorada por sistemas que verificam os principais serviços e servidores, emitindo alertas caso identifique algum problema de performance e/ou inatividade.

4.6.11.4 Os recursos listados no inventário de ativos tecnológicos devem ser mantidos em condições adequadas de funcionamento.

4.6.11.5 Os ativos tecnológicos externos são controlados conforme diretrizes estabelecidas em contratos com os fornecedores.

4.6.12 **Acesso Remoto**

4.6.12.1 Todo o acesso remoto aos sistemas do CAP é feito, obrigatoriamente, através de VPN (*Virtual Private Network*).

4.6.12.2 Todo equipamento que necessite acessar a rede do CAP remotamente deve possuir *software* cliente de VPN homologado, e será autorizado e monitorado pelo Departamento de Tecnologia da Informação.

4.6.12.3 Todo o gerenciamento desse processo é regulado conforme o PPTI 02 - Acesso Remoto.

4.6.13 **Acordos de Confidencialidade**

4.6.13.1 Acordos de confidencialidade deverão ser firmados com os colaboradores e prestadores de serviços ligados aos ativos relevantes para a segurança da informação.

4.6.14 **Relacionamento da Cadeia de Fornecimento**

4.6.14.1 Foram definidos processos para orientar os fornecedores do CAP que possuem relação com os ativos de informação sobre as diretrizes de segurança da informação, bem como conscientizá-los sobre o correto uso dos recursos da organização.

4.6.14.2 As instruções e regras protegem os ativos de informações disponibilizadas pelo CAP, assim como a segurança dos recursos tecnológicos, ambientes e dependências acessados pelos fornecedores, garantindo a correta custódia e prevenindo ameaças deliberadas ou acidentais.

4.6.15 **Gestão de Incidentes**

4.6.15.1 Promover um ambiente onde todos se comprometem com segurança da informação é extremamente importante e exige um processo contínuo de conscientização.

4.6.15.2 É responsabilidade de todos informarem possíveis violações das Diretrizes de Segurança da Informação.

4.6.15.3 O documento PPTI 07 - Gestão de Incidentes, estabelece as diretrizes para investigação e tratamento de incidentes.

4.6.16 **Conscientização, Educação e Treinamento**

4.6.16.1 Etapa responsável por realizar ações de conscientização, educação e treinamento em segurança da informação. Nesta etapa são realizadas as atividades:

a) Elaboração de estratégias para realização de campanhas de conscientização, educação e treinamento sobre a importância da segurança da informação;

b) Realização de ações de conscientização sobre segurança da informação, por meio de divulgação de materiais eletrônicos e/ou impressos;

c) Treinamentos com usuários sobre práticas seguras de privacidade e proteção de dados de forma presencial e/ou online; e

d) Disponibilização de materiais educativos sobre segurança da informação através dos canais de comunicação oficiais do CAP.

4.6.17 **Controle de Segurança**

4.6.17.1 Etapa responsável por realizar as implementações dos controles de segurança da informação, tais como: criptografia para proteger dados confidenciais em trânsito e em repouso, implementação de *softwares* de proteção de equipamentos e redes, dentre outras atividades.

4.6.17.2 Nesta etapa são realizadas as atividades:

a) Implementação de criptografia nos recursos, sistemas operacionais, sistemas de informação e aplicativos;

b) Instalação e configuração de antivírus nos ativos corporativos;

c) Instalação e configuração de sistemas prevenção e detecção de intrusão;

d) Instalação e configuração de controles de proteção relacionados ao uso de sistemas operacionais e *softwares* institucionais.

4.6.18 **Controle de Privacidade**

4.6.18.1 Etapa responsável por realizar as implementações dos controles de privacidade.

4.6.18.2 Nesta etapa são realizadas as atividades:

a) Identificação e classificação dos dados pessoais e sensíveis para garantir seu tratamento adequado;

b) Configuração de mecanismos de controle de acesso a dados sensíveis.

4.6.19 **Conformidade Regulatória**

4.6.19.1 Etapa responsável pela garantia de que o plano de gestão de segurança da informação esteja em conformidade com regulamentos de privacidade, como a LGPD, entre outros.

4.6.19.2 Nesta etapa são realizadas as atividades:

a) Avaliações de conformidade utilizando como parâmetros a legislação pertinente à privacidade e segurança da informação;

b) Elaboração de relatórios de conformidade exigidos por regulamentações específicas.

4.6.20 **Melhoria Contínua**

4.6.20.1 Etapa responsável por realizar a análise crítica dos resultados obtidos através da execução das etapas anteriores.

4.6.20.2 Nesta etapa são realizadas as atividades:

a) Revisão das políticas, programa, processos, normas, planos, procedimentos, contratos, acordos envolvendo privacidade e segurança da informação de acordo com a legislação pertinente;

b) Adaptação do plano de gestão de privacidade e segurança da informação de acordo com as ameaças cibernéticas, vulnerabilidades, tecnologias e regulamentos.

5. VIGÊNCIA

5.1 A presente Resolução Normativa entrará em vigor após sua aprovação em reunião da Diretoria.

Aprovação

_____

Gil Ferrari Bacos

Presidente da Diretoria

Resolução Normativa elaborada pela Comissão de Normatização

Beatriz Maria de Castro Oliveira (Presidente)

Geraldo Santamaria Filho

Maria José Nascimento Corrêa