POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

- PROGRAMA DE GOVERNANÇA EM PRIVACIDADE SMARTSYSTEMIT –

HISTÓRICO DE VERSÕES

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	Código: PSI	
Documento desenvolvido pela Paliares & Sanchotene Advogados Associados especificamente para SMARTSYSTEMIT.	Data de Criação: 04/04/2024	Versão: 00
Revisão PS Advogados Associados	Data de Revisão 15/07/2024	Versão: 01

SUMÁRIO

A SMARTSYSTEMIT SOLUÇÕES EM INFORMÁTICA LTDA **(“**SMARTSYSTEMIT**”)** possui o compromisso de resguardar e proteger as informações e os dados, sejam eles pessoais ou não, que estão sob sua guarda.

Nesse contexto, a segurança da informação é uma atividade essencial de proteção de todos os ativos tangíveis e intangíveis da SMARTSYSTEMIT.

Dessa forma, diante ao nosso programa de governança em privacidade, a presente POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (“Política”) apresenta diretrizes gerais de conduta, bem como obrigações a serem seguidas na SMARTSYSTEMIT a fim de mitigar eventuais riscos e danos relacionados a ameaças externas ou internas, deliberadas ou acidentais, que possam impactar na confidencialidade, integridade, disponibilidade, autenticidade e legalidade das informações de qualquer natureza.

Esta Política está de acordo com as leis vigentes em nosso país, bem como está alicerçada nas recomendações das normas técnicas ABNT NBR ISO/IEC 27001:2013 Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos, ABNT NBR ISO/IEC 27002:2013 — Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação e ABNT NBR ISO/IEC 27003:2020 — Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Orientações.

Assim sendo, a alta gestão da SMARTSYSTEMIT, está comprometida e apoia as diretrizes e obrigações estabelecidas nesta Política.

1. OBJETIVOS E APLICABILIDADE

A presente Política é um normativo interno, com valor jurídico e aplicabilidade imediata e irrestrita a todos os destinatários, que venham a ter acesso e/ou utilizam as informações, os recursos de TIC e/ou demais ativos tangíveis ou intangíveis da SMARTSYSTEMIT, tendo como objetivo:

i. Criar e estabelecer condições para que a SMARTSYSTEMIT eleve continuamente a sua maturidade em segurança da informação por meio da adoção de diretrizes, normas e procedimentos destinados a proteger os ativos de informação da SMARTSYSTEMIT, visando a promoção da Confidencialidade, Integridade, Disponibilidade, Autenticidade e Legalidade de tais ativos;

ii. Definir os parâmetros para normatização das questões de segurança da informação na SMARTSYSTEMIT;
iii. Descrever as regras comportamentais e procedimentos a serem seguidas na condução das atividades desenvolvidas pela SMARTSYSTEMIT, buscando garantir a prevenção de incidentes de segurança da informação e a proteção de dados pessoais.
iv. Estabelecer as linhas que assegurem e reforcem o compromisso da SMARTSYSTEMIT com as práticas e medidas preventivas garantidoras de segurança da informação.
v. Estabelecer as responsabilidades e limites de atuação dos destinatários em relação à segurança da informação e comunicação, reforçando uma cultura interna baseada em integridade.
vi. Prover a SMARTSYSTEMIT de mecanismos de atendimento e conformidade às leis de segurança da informação, nacionais e internacionais.

Esta Política estabelece os preceitos para garantir que seus destinatários entendam e cumpram as leis de proteção de dados pessoais, bem como os padrões e medidas técnicas que visam a segurança da informação da SMARTSYSTEMIT.

Assim, a presente Política se aplica a alta gestão, colaboradores, prestadores de serviços, fornecedores e terceiros (outros contratados e subcontratados pela SMARTSYSTEMIT), que atuem em nome da SMARTSYSTEMIT ("DESTINATÁRIOS"), e que, no âmbito dessa relação, possam acessar as áreas, equipamentos, informações, arquivos, redes e dados de titularidade, propriedade ou em posse da SMARTSYSTEMIT.

Desta forma, todos os destinatários deverão observar as presentes regras e recomendações em quaisquer operações ou processos que possam impactar na segurança da informação da SMARTSYSTEMIT.

O não cumprimento das disposições ora previstas, sujeitará o "infrator" às sanções fixadas nesta Política, sem prejuízo das medidas previstas em lei, caso se aplique.

Ademais, é obrigação de cada destinatário manter-se atualizado em relação a esta Política e aos procedimentos e normas relacionadas, buscando orientação sempre que não estiver absolutamente seguro quanto à aquisição, uso e/ou descarte de informações, recursos de TIC e/ou demais ativos tangíveis ou intangíveis da SMARTSYSTEMIT.

2. PRINCÍPIOS

O compromisso da SMARTSYSTEMIT com o tratamento adequado das informações se baseia nos seguintes princípios:

i. **Confidencialidade** – o acesso à informação é permitido somente para pessoas autorizadas e quando ele for estritamente necessário.
ii. **Integridade** – todos os esforços serão feitos para que as informações sejam exatas e completas, bem como seu processamento.
iii. **Disponibilidade** – sempre que necessário, as pessoas autorizadas terão acesso às informações.
iv. **Autenticidade** – todos os esforços serão feitos para que as informações sejam confiáveis e corretas, ou seja, as informações não serão alteradas de forma não autorizada ou indevida.
v. **Legalidade** – todos os esforços serão feitos para assegurar que todos os procedimentos relacionados às informações dentro da empresa sejam feitos de acordo com a lei.

Ou seja, a SMARTSYSTEMIT buscará sempre preservar e proteger as informações sob a responsabilidade, inclusive as contidas nos recursos de Tecnologia da Informação e Comunicação ("TIC"), dos diversos tipos de ameaça e desvios de finalidade em todo o seu ciclo de vida, estejam elas em qualquer suporte ou formato. Prevenindo e mitigando impactos gerados por incidentes envolvendo a segurança da informação e comunicação.

Assegurando no desenvolvimento das atividades do negócio a real observância de tais princípios. Cumprindo a legislação vigente no Brasil e demais instrumentos regulamentares relacionados às atividades da SMARTSYSTEMIT no que diz respeito à segurança da informação, aos objetivos institucionais dentro dos pilares morais, éticos e de privacidade.

3. TERMOS E DEFINIÇÕES

Para efeito desta Política, são adotados as siglas, os termos e definições constantes a seguir:

i. **Ameaça**: qualquer circunstância ou evento com o potencial de causar impacto negativo sobre a confidencialidade, integridade, autenticidade e disponibilidade da informação;
ii. **Assinatura digital**: conjunto de dados criptografados, associados a determinado documento ou arquivo que foi assinado, destinado a garantir a autenticidade e a integridade das informações constantes do documento, sua autoria e eventuais modificações;
iii. **Acessibilidade**: facilidade no acesso ao conteúdo e ao significado de um objeto digital;

iv. **Ativo de informação**: patrimônio composto de dados, informações e conhecimentos obtidos, gerados e manipulados durante a execução dos sistemas e processos de trabalho;

v. **Metadados**: dados estruturados que descrevem e permitem encontrar, gerenciar, compreender e/ou preservar documentos arquivísticos ao longo do tempo;

vi. **Autenticidade**: propriedade de que a informação foi produzida, expedida, modificada ou destruída por um determinado indivíduo, entidade ou processo;

vii. **Banco de Dados (ou Base de Dados)**: um sistema de armazenamento de dados, ou seja, um conjunto de registros que tem como objetivo organizar e guardar as informações;

viii. **Confidencialidade**: propriedade de que a informação não será disponibilizada ou divulgada a indivíduos, entidades ou processos sem autorização;

ix. **Cópia de Segurança (backup)**: guarda de dados em um meio separado do original, de forma a protegê-los de qualquer eventualidade.

x. **Fidedignidade**: credibilidade de um documento arquivístico como uma afirmação do fato. Existe quando um documento arquivístico pode sustentar o fato ao qual se refere e é estabelecida pelo exame da completeza, da forma do documento e do grau de controle exercido no processo de sua produção;

xi. **Computação em nuvem**: modelo computacional que permite acesso, por demanda e independentemente da localização, a conjunto compartilhado de recursos configuráveis de computação (rede de computadores, servidores, armazenamento, aplicativos e serviços), provisionados com esforços mínimos de gestão ou interação com o provedor de serviços;

xii. **Controle de acesso**: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso;

xiii. **Custódia**: responsabilidade jurídica de guarda e proteção de arquivos, independentemente de vínculo de propriedade.

xiv. **Custodiante da informação**: usuário que atua em uma ou mais fases do tratamento da informação, ou seja, recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação, incluindo a sigilosa;

xv. **Disponibilidade**: propriedade de que a informação esteja acessível e utilizável sob demanda por indivíduo, entidades ou processos;

xvi. **Dispositivos móveis**: equipamentos portáteis, dotados de capacidade computacional e dispositivos removíveis de memória para armazenamento, entre eles, notebooks, netbooks, smartphones, tablets, pen drives, USB drives, HD externos e cartões de memória;

xvii. **Gestor de Privacidade**: pessoa designada com a responsabilidade de receber, analisar e responder a notificações e atividades relacionadas a incidentes de segurança; Responsável pelas ações de segurança da informação no âmbito da SMARTSYSTEMIT;

xviii. **Evento**: Acontecimento que acarrete a mudança do estado atual de um processo;

xix. **Gestão de continuidade**: processo abrangente de gestão que identifica ameaças potenciais para uma organização e os possíveis impactos nas finalidades institucionais, caso essas ameaças se concretizem. Esse processo fornece estrutura para que se desenvolva uma resiliência organizacional capaz de responder efetivamente e salvaguardar os interesses das partes envolvidas, a reputação e a marca da organização, assim como seus processos e seu valor agregado. É o resultado da fusão dos Planos de Contingência e dos Planos de Recuperação de Desastres, que objetiva garantir a recuperação de um ambiente de produção, independentemente de eventos que suspendam suas operações e de danos nos componentes (processos, pessoas, softwares, hardwares, infraestrutura, etc.) por ele utilizados;

xx. **Gestão de Segurança da Informação**: ações e métodos que visam à integração das atividades de gestão de riscos, tratamento de incidentes, tratamento da informação, conformidade, credenciamento, segurança cibernética, segurança física, segurança lógica, segurança orgânica e segurança organizacional aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto, à Tecnologia da Informação;

xxi. **Gestão de Riscos em Segurança da Informação**: conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos;

xxii. **Incidente de segurança**: evento ou conjunto de eventos de segurança da informação, indesejados ou inesperados, confirmados ou sob suspeita, que tenham grande probabilidade de comprometer as operações e ameaçar a segurança da informação;

xxiii. **Informação**: conjunto de dados, textos, imagens, métodos, sistemas ou quaisquer formas de representação dotadas de significado em determinado contexto, independentemente do meio em que resida ou da forma pela qual seja veiculado;

xxiv. **Integridade**: propriedade de que a informação não foi modificada ou destruída, de maneira não autorizada ou acidental, por indivíduos, entidades ou processos;

xxv. **Documento arquivístico**: documento produzido ou recebido no curso de uma atividade prática como instrumento ou resultado dessa atividade, retido para ação ou referência;

xxvi. **Inventário e Mapeamento de Ativos de Informação**: processo interativo e evolutivo, composto de três etapas:

a) identificação e classificação de ativos de informação;

b) identificação de potenciais ameaças e vulnerabilidades; e
c) avaliação de riscos.

xxvii. **Malwares**: o nome malware vem do inglês malicous software (programa malicioso). Refere-se a qualquer tipo de programa indesejado, instalado sem seu consentimento e que pode trazer danos ao seu dispositivo;

xxviii. **Preservação digital**: conjunto de ações gerenciais e técnicas exigidas para superar as mudanças tecnológicas e a fragilidade dos suportes, garantindo o acesso e a interpretação de documentos digitais pelo tempo que for necessário;

xxix. **Repositório digital**: complexo que apoia o gerenciamento dos materiais digitais, pelo tempo que for necessário, e é formado por elementos de hardware, software e metadados, bem como por uma infraestrutura organizacional e procedimentos normativos e técnicos;

xxx. **Repositório arquivístico digital**: repositório digital que armazena e gerencia documentos arquivísticos, seja nas idades corrente e intermediária, seja na idade permanente;

xxxi. **Plano de Continuidade de Serviços Essenciais**: documentação dos procedimentos e informações necessários para manter os ativos de informação críticos e a continuidade de suas atividades em local alternativo previamente definido, em casos de incidentes;

xxxii. **Plano de Recuperação de Serviços Essenciais**: documentação dos procedimentos e informações necessários para que se operacionalize o retorno das atividades críticas à normalidade;

xxxiii. **Política de Segurança da Informação**: documento aprovado pela autoridade responsável pela empresa, com objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação.

xxxiv. **Público-Alvo**: conjunto de usuários internos e externos atendidos pela Equipe de Tratamento e Resposta a Incidentes;

xxxv. **Recurso Criptográfico**: sistemas, programas, processos e equipamento isolado ou em rede que utiliza algoritmo simétrico ou assimétrico para realizar a cifração ou decifração;

xxxvi. **Risco**: possibilidade potencial de uma ameaça comprometer a informação ou o sistema de informação pela exploração da vulnerabilidade;

xxxvii. **Segurança da Informação**: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

xxxviii. **Serviços Essenciais**: são aqueles que são imprescindíveis à atividade finalística da empresa;

xxxix. **Spam**: termo usado para referir-se a e-mails não solicitados, que geralmente são enviados para um grande número de pessoas.

xl. **Termo de Responsabilidade**: termo assinado pelo usuário concordando em contribuir com a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações que tiver acesso, bem como assumir responsabilidades decorrentes de tal acesso;

xli. **Termo de Confidencialidade**: documento formal assinado por colaboradores, terceiros, estagiários e prestadores de serviço da SMARTSYSTEMIT, por meio do qual se comprometem a manter sigilo em relação às informações consideradas confidenciais e respeitar as normas de segurança vigentes;

xlii. **Tratamento da informação**: recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação, inclusive as sigilosas;

xliii. **Trilhas de Auditoria**: são rotinas específicas programadas nos sistemas para fornecerem informações de interesse da auditoria. São entendidas como o conjunto cronológico de registros (logs) que proporcionam evidências do funcionamento do sistema. Esses registros podem ser utilizados para reconstruir, rever/revisar e examinar transações desde a entrada de dados até a saída dos resultados finais, bem como para avaliar/rastrear o uso do sistema, detectando e identificando usuários não autorizados;

xliv. **Unidades Organizacionais**: unidade em que está lotado o colaborador, terceirizado, estagiário ou aprendiz;

xlv. **Usuários**: pessoa física ou jurídica que opera algum sistema informatizado da SMARTSYSTEMIT;

xlvi. **Vulnerabilidade**: fragilidade de um ativo ou grupo de ativos de informação que pode ser explorada negativamente por uma ou mais ameaças;

xlvii. **Phishing**: também conhecido como roubo de identidade. É uma fraude eletrônica, na qual o criminoso cibernético tenta obter informações confidenciais de forma fraudulenta. Normalmente, é realizado por falsificação de e-mail ou mensagem instantânea, e, muitas vezes, direciona usuários a inserir informações pessoais em um site falso, que corresponde à aparência do site legítimo. Esse método é muito usado para roubar senhas e números de cartões de crédito, entre outros dados confidenciais.

4. CLASSIFICAÇÃO DA INFORMAÇÃO

A classificação e o tratamento da informação, realizados por meio de procedimento definido, abrange informações provenientes dos serviços desenvolvidos pela SMARTSYSTEMIT.

As informações devem ser classificadas de forma a permitir tratamento diferenciado de acordo com o seu grau de importância, criticidade, sensibilidade e em conformidade com requisitos legais.

As informações devem ser classificadas e identificadas por rótulos, considerando os seguintes níveis:

i. **Pública**: são informações explicitamente aprovadas por seu responsável para consulta irrestrita e cuja divulgação externa não compromete a execução das finalidades institucionais e que, por isso, não necessitam de proteção efetiva ou tratamento específico;
ii. **Interna**: são informações disponíveis aos colaboradores da SMARTSYSTEMIT para a execução de suas tarefas rotineiras, não se destinando, portanto, ao uso do público externo;
iii. **Confidencial**: são informações de acesso restrito a um colaborador ou grupo de colaboradores. Sua revelação pode violar a privacidade de indivíduos, violar acordos de confidencialidade, dentre outros;
iv. **Confidencial/Restrita**: são informações de acesso restrito a um colaborador ou grupo de colaboradores que, obrigatoriamente, são delas destinatários. Em geral, informações associadas ao interesse estratégico da SMARTSYSTEMIT e estão restritas a alta gestão, ao(à) diretor(a), aos coordenadores, aos gerentes e aos colaboradores, cujas funções requeiram conhecê-las, em especial, resultado da avaliação de desempenho.

5. COMPETÊNCIAS

A Gestor de privacidade compete:

i. propor melhorias e atualizar a Política de Segurança da Informação (PSI);
ii. propor, analisar e revisar normas complementares relativas à segurança da informação, em conformidade com as legislações vigentes e submeter à aprovação da alta gestão da SMARTSYSTEMIT;
iii. tratar dos assuntos de Segurança da Informação e assessorar diretamente as decisões da alta gestão da SMARTSYSTEMIT;
iv. propor investimentos relacionados à segurança da informação com o intuito de fortalecer o ambiente tecnológico e não digital e minimizar os riscos causados em virtude de possíveis vulnerabilidades;
v. classificar e reclassificar o nível de acesso às informações sempre que necessário;
vi. acompanhar o gerenciamento do ciclo de vida de incidentes de segurança, visando ao processo de melhoria contínua;
vii. coordenar as atividades de tratamento e resposta a incidentes de segurança;
viii. agir proativamente com o objetivo de evitar que ocorram incidentes de segurança, divulgando práticas e recomendações de Segurança da Informação e avaliando condições de segurança de rede por meio de verificações de conformidade;

ix. executar as ações necessárias para tratar quebras de segurança;
x. obter informações quantitativas acerca dos incidentes ocorridos que descrevam sua natureza, causas, data de ocorrência, frequência e custos resultantes.
xi. planejar e coordenar a execução das ações de Segurança da Informação;
xii. definir estratégias para a implementação desta Política de Segurança da Informação (PSI) e suas normas complementares;
xiii. acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança e adotar as medidas administrativas necessárias à aplicação de ações corretivas;
xiv. gerenciar a análise de risco;
xv. verificar se os procedimentos de Segurança da Informação estão sendo aplicados de forma a atender à conformidade com legislações vigentes; e
xvi. providenciar a divulgação interna e permanente desta PSI e de suas normas complementares.

Ao Departamento de TI compete:

i. planejar, coordenar, supervisionar, executar e controlar as atividades de TI em conformidade com as diretrizes desta PSI;
ii. elaborar, implementar e atualizar normas internas específicas em conformidade com esta PSI e demais diretrizes da alta gestão;
iii. propor as metodologias e processos referentes à segurança da informação, como classificação de acessos à informação, avaliação de risco, análise de vulnerabilidade, entre outros;
iv. gerenciar o ciclo de vida de incidentes de segurança, visando ao processo de melhoria contínua;
v. manter registros e procedimentos como trilhas de auditoria e outros que assegurem o rastreamento, o acompanhamento, o controle e a verificação de acesso a todos os sistemas corporativos e das redes computacionais da SMARTSYSTEMIT;
vi. supervisionar os acessos às informações e aos ativos de tecnologia (sistemas, banco de dados, recursos de rede), tendo como referência a PSI e as normas de segurança da informação;
vii. efetuar as alterações, exclusões, inclusões e manter registro e controles atualizados de todos os acessos sempre que demandado formalmente pelas Unidades Organizacionais acerca de admissão, demissão e movimentação de pessoal e/ou entrada/saída de novos processos;

Ao Departamento de Recursos Humanos (área de Pessoal) compete:

i. comunicar ao Departamento de Tecnologia da Informação o ingresso, a alteração de lotação ou localização, bem como o desligamento de pessoal, inclusive postos terceirizados, no âmbito da SMARTSYSTEMIT.

6. RESPONSABILIDADE

No âmbito da SMARTSYSTEMIT os usuários têm as seguintes responsabilidades:

i. ter pleno conhecimento e cumprir fielmente a PSI, as normas e os procedimentos de segurança da informação da SMARTSYSTEMIT;
ii. solicitar esclarecimentos ao Gestor de Privacidade em caso de dúvidas relacionadas à PSI;
iii. gerenciar os ativos sob sua responsabilidade e garantir que os documentos e arquivos impressos ou digitais, equipamentos e recursos tecnológicos à sua disposição sejam utilizados, exclusivamente, para uso a serviço da SMARTSYSTEMIT;
iv. acessar a rede de dados da SMARTSYSTEMIT somente após tomar ciência das normas de Segurança da Informação e assinar o Termo de Responsabilidade;
v. tratar a informação arquivística digital e impressa como patrimônio da SMARTSYSTEMIT e como recurso que deva ter seu sigilo preservado;
vi. utilizar as informações arquivísticas digitais e impressas disponibilizadas e os sistemas e produtos computacionais de propriedade ou direito de uso da SMARTSYSTEMIT exclusivamente para o interesse do serviço;
vii. preservar o conteúdo das informações sigilosas a que tiver acesso, sem divulgá-las para pessoas não autorizadas e/ou que não tenham necessidade de conhecê-las;
viii. não tentar obter acesso à informação cujo grau de sigilo não seja compatível com a sua Credencial de Segurança ou cujo teor não tenha autorização ou necessidade de conhecer;
ix. não se fazer passar por outro usuário usando a identificação com login e senha de acesso;
x. no caso de demissão, licenciamento, término de prestação de serviço ou qualquer tipo de afastamento, preservar o sigilo das informações e documentos sigilosos a que teve acesso;
xi. não compartilhar, transferir, divulgar ou permitir o conhecimento de credenciais de acesso (senhas) utilizadas no ambiente computacional da SMARTSYSTEMIT por terceiros;
xii. responder perante a SMARTSYSTEMIT pelo uso indevido das suas credenciais de acesso, no âmbito administrativo e, se for o caso, perante a Justiça, no âmbito penal e civil;
xiii. não transmitir, copiar ou reter arquivos contendo textos, fotos, filmes ou quaisquer outros registros que contrariem a moral, os bons costumes e a legislação vigente;
xiv. não transferir qualquer tipo de arquivo que pertença a SMARTSYSTEMIT para outro local, seja por meio magnético ou não, exceto no interesse do serviço e mediante autorização da autoridade competente;

xv. estar ciente de que o processamento, o trâmite e o armazenamento de arquivos que não sejam de interesse do serviço não são permitidos na rede computacional da SMARTSYSTEMIT;

xvi. estar ciente de que toda informação digital armazenada, processada e transmitida no ambiente computacional e nos arquivos setoriais, intermediários e permanentes impressos ou digitais da SMARTSYSTEMIT pode ser auditada;

xvii. estar ciente de que o correio eletrônico é de uso exclusivo para o interesse do serviço e que qualquer correspondência eletrônica originada ou retransmitida no ambiente computacional da SMARTSYSTEMIT deve obedecer a esse preceito;

xviii. assinar o Termo de Responsabilidade e declarar, formalmente, ter pleno conhecimento e aceitar expressamente, sem reservas, os termos desta PSI;

xix. utilizar as credenciais de acesso, login e senha, e os recursos computacionais, em conformidade com a PSI da SMARTSYSTEMIT e procedimentos estabelecidos em normas específicas do programa de governança em privacidade;

xx. comunicar, tempestivamente, ao gestor imediato ou ao Gestor de Privacidade qualquer violação a esta política, suas normas e procedimentos;

xxi. fazer uso da política de mesa limpa e tela protegida para garantir a proteção das informações de maneira eficaz e reduzir os riscos de acesso não autorizado, perda ou dano à informação durante e fora do horário normal de trabalho.

xxii. devolução das informações ou documentos sigilosos que estejam em seu poder

xxiii. eliminação completa de dados digitais que porventura foram armazenados em seus equipamentos eletrônicos e softwares de uso particular e e-mails pessoais.

Ao Custodiante da Informação cabem as seguintes responsabilidades:

i. cumprir e zelar pela observância integral das diretrizes desta PSI e demais normas e procedimentos decorrentes;

ii. zelar pela disponibilidade, integridade e confidencialidade das informações e recursos em qualquer suporte sob sua custódia, conforme condições estabelecidas nesta PSI e demais normas e procedimentos decorrentes, mediante assinatura do Termo de Responsabilidade;

iii. participar de capacitação e treinamento em segurança da informação, quando convocado;

iv. utilizar os recursos sob sua responsabilidade, exclusivamente, para o fim a que se destinam;

v. proteger as informações contra acesso, modificação, destruição ou divulgação não autorizada;

vi. preservar a classificação do grau de sigilo de documentos, dados e informações dos quais tiver conhecimento em decorrência do exercício de suas funções; e

vii. comunicar prontamente ao seu gestor imediato e ao Comitê de Segurança da Informação qualquer incidente de que tenha conhecimento ou situações que comprometam a disponibilidade, a integridade e a confidencialidade das informações.

7. DIRETRIZES

Esta Política tem como principal diretriz a preservação da disponibilidade, integridade e confiabilidade dos dados, informações e conhecimentos que compõem o ativo da informação da SMARTSYSTEMIT.

Os usuários deverão ser treinados e conscientizados nos procedimentos de segurança da informação.

Quando do afastamento, da mudança de responsabilidade, de lotação ou de atribuições do usuário dentro da organização, far-se-á necessária a revisão imediata dos direitos de acesso e uso dos ativos.

Os direitos de acesso e o uso dos ativos atribuídos ao usuário deverão ser extintos quando da efetivação de seu desligamento.

Todo ativo produzido pelo usuário desligado será de propriedade da SMARTSYSTEMIT, observadas as disposições da legislação aplicável.

Esta Política de Segurança da Informação é constituída dos seguintes pressupostos básicos:

i. o sucesso das ações nos assuntos de segurança da informação está diretamente associado à capacitação científico-tecnológica dos recursos humanos envolvidos, à conscientização do público interno, à qualidade das soluções adotadas e à proteção das informações contra ameaças internas e externas;
ii. a informação é um recurso vital para o adequado funcionamento de toda e qualquer organização, devendo ser tratada como patrimônio a ser protegido e preservado;
iii. a Política de Segurança da Informação é o instrumento que regula a proteção dos dados, informações e conhecimentos da Instituição, com vistas à garantia de integridade, de disponibilidade e de confidencialidade;
iv. todos os colaborador, estagiários, e prestadores de serviços, que, oficialmente, execute atividade vinculada à atuação institucional da SMARTSYSTEMIT e sejam usuários dos ativos sigilosos devem assinar o Termo de Responsabilidade quanto ao sigilo dos dados, informações e conhecimentos da administração da SMARTSYSTEMIT.

8. TRATAMENTO DA INFORMAÇÃO

Esta Política de Segurança da Informação considera os seguintes requisitos para o Tratamento da Informação:

i. toda informação criada, adquirida ou custodiada pelo usuário, no exercício de suas atividades, é considerada bem e propriedade da SMARTSYSTEMIT e deve ser protegida segundo as diretrizes descritas nesta PSI e demais regulamentações em vigor, com o objetivo de minimizar riscos às atividades e serviços institucionais e preservar sua imagem;
ii. é expressamente proibido o acesso, a guarda ou o encaminhamento de material discriminatório, malicioso, não ético, obsceno ou ilegal por intermédio de quaisquer meios e recursos de tecnologia da informação disponibilizados pela SMARTSYSTEMIT;
iii. os ativos de informação devem ser protegidos de forma preventiva, com o objetivo de minimizar riscos às atividades e aos objetivos das finalidades institucionais da SMARTSYSTEMIT;
iv. as informações criadas, armazenadas, manuseadas, transportadas ou descartadas devem ser classificadas segundo o grau de sigilo, criticidade e outros, conforme normas internas e legislação específica em vigor;
v. todo usuário deve respeitar a classificação atribuída a uma informação e, a partir dela, conhecer e obedecer às restrições de acesso e divulgação associadas;
vi. as informações produzidas ou custodiadas pela SMARTSYSTEMIT somente devem ser descartadas ou destruídas conforme o seu nível de classificação e atendendo às exigências legais;
vii. deve ser disponibilizada uma solução de Gestão Eletrônica de Documentos com mecanismos de assinatura digital aderente à legislação em vigor, com a finalidade de mitigar riscos associados à informação impressa;
viii. a manipulação de informações classificadas em qualquer grau de sigilo deve seguir as normas internas e a legislação em vigor;

Qualquer outra forma de uso das informações que extrapole as atribuições necessárias ao desempenho das atividades dos usuários, internos ou colaboradores, necessitará de prévia autorização formal.

O acesso, quando autorizado, dos usuários internos ou externos às informações produzidas ou custodiadas pela SMARTSYSTEMIT, que não sejam de domínio público, será condicionado a um termo de sigilo e responsabilidade, formal ou virtual.

As informações deverão ser classificadas de forma a permitir tratamento diferenciado de acordo com seu grau de importância, criticidade, sensibilidade, e em conformidade com requisitos legais.

9. UTILIZAÇÃO DA REDE

O ingresso à rede interna deve ser devidamente controlado para que os riscos de acessos não autorizados e/ou indisponibilidade das informações sejam minimizados, devendo os procedimentos serem definidos em normas específicas, em especial, a Política de Controle de Acesso Lógico da SMARTSYSTEMIT.

10. TRATAMENTO INCIDENTES DE REDE

A gestão de incidentes de segurança da informação deverá ser realizada por meio de processo formalizado, contendo as fases de detecção, triagem, análise e resposta aos incidentes de segurança.

Departamento de Tecnologia da Informação (DTI) manterá a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais, com a responsabilidade de receber, analisar e responder a notificações e a atividades relacionadas a incidentes de segurança em rede de computadores.

11. GESTÃO DE RISCOS

A gestão de riscos é realizada por meio de processo formalizado, contendo as fases de análise, avaliação e tratamento dos riscos.

Os riscos devem ser continuamente monitorados e tratados, de acordo com as vulnerabilidades associadas aos ativos de informação e aos níveis de risco, conforme procedimentos definidos em norma específica sobre gestão de riscos em segurança da informação.

Os usuários são responsáveis por adotar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos seus ativos de informação no âmbito da SMARTSYSTEMIT.

O processo de inventário e mapeamento de ativos de informação deve ser aplicado tanto na gestão de riscos quanto na gestão de continuidade.

12. GESTÃO DE CONTINUIDADE

A SMARTSYSTEMIT deve manter processo de gestão de continuidade das atividades e processos críticos, visando não permitir que estes sejam interrompidos e assegurar a sua retomada em tempo hábil.

As informações de propriedade ou custodiadas pela SMARTSYSTEMIT, quando armazenadas em meio eletrônico, devem ser providas de cópia de segurança atualizada e guardada em local remoto, de forma a garantir a continuidade das atividades empresariais.

As informações armazenadas em outros meios devem possuir mecanismos de proteção que preservem sua integridade, conforme o nível de classificação atribuído.

As diretrizes para a Gestão de Continuidade de TI em Segurança da Informação, deve minimizar os impactos decorrentes de falhas, desastres ou indisponibilidades significativas sobre as atividades críticas, além de recuperar perdas de ativos de informação em nível aceitável, por intermédio de ações de prevenção, resposta e recuperação.

13. AUDITORIA E CONFORMIDADE

A Auditoria em Segurança da Informação é uma atividade devidamente estruturada para examinar criteriosamente a situação dos controles que se aplicam à segurança da informação, especialmente por meio da análise de objetos e respectivos pontos de controle.

Para tanto, é preciso verificar que os controles estejam de acordo com as normas e políticas de segurança estabelecidas para esses ativos, bem como se o que está em operação alcança os objetivos de segurança.

A SMARTSYSTEMIT deve criar e manter registros e procedimentos, como trilhas de auditoria, que possibilitem o rastreamento, o acompanhamento, o controle e a verificação de acessos aos sistemas corporativos e rede interna da empresa.

Deve ser realizada, com periodicidade mínima anual, verificação de conformidade das práticas de Segurança da Informação aplicadas na SMARTSYSTEMIT com esta PSI, bem como com a legislação específica em vigor.

A verificação de conformidade deve ser realizada nos contratos, convênios, acordos de cooperação e outros instrumentos do mesmo gênero celebrados com a SMARTSYSTEMIT.

A verificação de conformidade poderá combinar ampla variedade de técnicas, tais como análise de documentos, análise de registros e logs, análise de código-fonte, entrevistas e testes de invasão;

Os resultados de cada ação de verificação de conformidade serão documentados em Relatório de Avaliação de Conformidade;

Os procedimentos e as metodologias utilizados na auditoria e conformidade no âmbito da SMARTSYSTEMIT devem estar em conformidade com as diretrizes desta PSI e demais legislações em vigor;

As medidas de proteção para que administradores de sistemas não tenham permissão de exclusão ou desativação de registros de log de suas próprias atividades deverão ser tomadas;

Os recursos e informações de registro de log deverão ser protegidos contra falsificação e acesso não autorizado.

14. CONTROLE DE ACESSO

O controle de acesso aos sistemas internos e externos, o credenciamento de acesso de usuários aos ativos de informação e o acesso às informações em áreas e instalações consideradas críticas devem ser implantados nos níveis físico e lógico, conforme Política de Controle de Acesso Lógico, e em conformidade com as diretrizes desta política.

As medidas de proteção serão adotadas para evitar que usuários dos ativos de Tecnologia da Informação não tenham permissão para instalar, remover, modificar, criar ou desenvolver softwares sem a devida autorização.

15. POLÍTICA DE SENHAS

A política de senhas de acessos aos sistemas e informações da SMARTSYSTEMIT deve ser definida em conforme Política de Controle de Acesso Lógico, e em conformidade com as diretrizes desta política.

16. USO DE E-MAIL

O uso de e-mail no âmbito da SMARTSYSTEMIT deve ser conforme Política de Controle de Acesso Lógico, e em conformidade com as diretrizes desta política.

17. ACESSO À INTERNET E INTRANET

O acesso à rede mundial de computadores, no âmbito da SMARTSYSTEMIT, deve ser conforme Política de Controle de Acesso Lógico, e em conformidade com as diretrizes desta política, além das orientações governamentais e legislações específicas em vigor.

18. INVENTÁRIO E MAPEAMENTO DE ATIVOS DE INFORMAÇÃO

Nos aspectos relacionados à Segurança da Informação, o processo de Inventário e Mapeamento de Ativos de Informação deve produzir subsídios para a Gestão de Segurança da Informação, Gestão de Riscos de Segurança da Informação, Gestão de Continuidade de TI, bem como para os procedimentos de avaliação da conformidade, de melhorias contínuas, de auditoria e, principalmente, de estruturação e de geração da base de dados sobre os ativos de informação.

O processo de Inventário e Mapeamento de Ativos de Informação deve ser dinâmico, periódico e estruturado, para manter a Base de Dados de Ativos de Informação atualizada e, consequentemente, prover informações para o desenvolvimento de ações e planos de aperfeiçoamento de práticas de Gestão da Segurança da Informação.

O inventário deve documentar e classificar a importância do ativo para as finalidades institucionais, o impacto para atividades finalísticas em caso de comprometimento e a estratégia que permita a recuperação do ativo em caso de desastre.

Todos os ativos críticos devem ter um proprietário formalmente designado.

O proprietário dos ativos de informação é a parte interessada da SMARTSYSTEMIT, ou indivíduo legalmente instituído por sua posição e/ou cargo, o qual é responsável primário pela viabilidade e sobrevivência dos ativos de informação.

O proprietário é responsável por:

a. assegurar que as informações e os ativos associados com os recursos de processamento da informação estejam adequadamente classificados;
b. definir e periodicamente analisar criticamente as classificações e as exigências de segurança da informação para os ativos de informação;
c. identificar os riscos e comunicar as exigências de segurança da informação para os ativos sob sua responsabilidade aos custodiantes e usuários;
d. implementar controles internos a fim de verificar se as exigências estão sendo cumpridas.

O proprietário do ativo pode delegar formalmente as tarefas de rotina a um custodiante que cuida do ativo no dia a dia, porém a responsabilidade permanece do proprietário.

O custodiante dos ativos de informação é qualquer indivíduo ou estrutura que tenha a responsabilidade formal de proteger um ou mais ativos de informação. É responsável por aplicar os níveis de controles de segurança em conformidade com as exigências de segurança da informação informadas pelo proprietário dos ativos de informação.

As regras para uso dos ativos associados com a informação e dos recursos de processamento da informação devem ser identificadas, documentadas e implementadas.

Os usuários que têm acesso aos ativos da SMARTSYSTEMIT devem estar conscientes dos requisitos de segurança da informação.

A informação deve ser classificada em termos do seu valor, requisitos legais, sensibilidade e criticidade para evitar modificação ou divulgação não autorizada.

O proprietário do ativo de informação deve ser responsável por sua classificação.

19. DISPOSITIVOS MÓVEIS

O uso de dispositivos móveis para acesso aos recursos computacionais no âmbito da SMARTSYSTEMIT deve ser controlado com a implementação de mecanismos de autenticação, autorização e registro de acesso do usuário, em conformidade com as diretrizes desta Política, bem como as demais legislações vigentes sobre o tema.

20. COMPUTAÇÃO EM NUVEM

A implementação ou contratação de computação em nuvem no âmbito da SMARTSYSTEMIT deve estar em conformidade com as diretrizes desta Política e com as demais legislações vigentes sobre o tema.

21. BACKUP

Todo sistema ou informação relevante para a operação das finalidades institucionais da SMARTSYSTEMIT deve possuir cópia dos seus dados de produção para que, em eventual incidente de indisponibilidade de dados, seja possível recuperar ou minimizar os impactos nas operações da instituição**.**

22. CONTRATAÇÃO DE SERVIÇOS

Nos contratos de empresas prestadoras de serviços com a SMARTSYSTEMIT, deverá constar cláusula específica sobre a obrigatoriedade de atendimento às normas desta Política, bem como ser exigida da empresa contratada e do prestador de serviços a assinatura do Termo de Responsabilidade e do Termo de Confidencialidade.

A empresa contratada também deverá demonstrar que possui mecanismos que assegurem a segurança das informações da SMARTSYSTEMIT por ela acessadas, direta ou indiretamente, acesso aos ativos que contêm informações, e cumprir o disposto nesta Política, quando aplicável.

23. DIVULGAÇÃO E ATUALIZAÇÃO

Esta Política e suas atualizações, após publicação, deverão ser amplamente divulgadas aos usuários, sendo consideradas um documento de relevante interesse público.

Esta Política de Segurança da Informação deverá ser revisada a cada 1 (um) ano ou sempre que se fizer necessário, não excedendo ao período máximo de 2 (dois) anos, a contar da data de sua publicação.

24. DISPOSIÇÕES FINAIS

A inobservância dos dispositivos constantes desta Política de Segurança da Informação pode acarretar, isolada ou cumulativamente, nos termos da lei, sanções administrativas, civis ou penais, assegurados aos envolvidos o contraditório e a ampla defesa.

Essa Política é parte do Programa de Governança e Proteção de Dados da SMARTSYSTEMIT e complementa demais normas e procedimentos vigentes.

Campinas, 04 de abril de 2024.

SMARTSYSTEMIT SOLUÇÕES EM INFORMÁTICA LTDA
Rua José Paulino, no 416, Sala 105, Centro, Campinas / SP
CEP: 13013-000
(19) 3236-1117