POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Versão 1.0

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO - SOCIN

Data deste documento:17/02/2022

ÍNDICE

1. Introdução

A SOCIN SOLUÇÕES COMERCIAIS INTEGRADAS LTDA (SOCIN), CNPJ 68.319.656/0001-05, desenvolveu a presente Política de Segurança da Informação (PSI) com fundamento na importância da implementação e manutenção da segurança de quaisquer tipos de ativos de informação necessários para o desenvolvimento de suas atividades empresariais. Nesse sentido, destacam-se os seus objetivos, sua abrangência, suas diretrizes, atribuições e princípios.

2. Objetivos

A presente PSI tem como objetivos:

2.1. Estabelecer diretrizes segurança da informação, visando estabelecer medidas e procedimentos em segurança da informação;

2.2. Promover, em relação à informação:

2.2.1. A Confidencialidade;

2.2.2. A Integridade; e

2.2.3. A Disponibilidade.

2.3. Definir e implementar práticas de proteção de diversos tipos de informações relevantes para o desenvolvimento de suas atividades empresariais, incluindo dados pessoais tratados pela SOCIN sob quaisquer bases legais, informações confidenciais e outras categorias de informações aplicáveis.

3. Abrangência

A presente PSI aplica-se a todos os usuários da SOCIN.

4. Diretrizes

4.1. A SOCIN considera que suas informações são bens valiosos. Seu uso está pautado na preservação de dados pessoais, em conformidade com a Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018), de seus:

4.1.1. Clientes;
4.1.2. Colaboradores;
4.1.3. Prestadores de serviços; e
4.1.4. Fornecedores.

4.2. A segurança da informação está baseada nos seguintes princípios:

4.2.1. Confidencialidade;
4.2.2. Integridade; e
4.2.3. Disponibilidade.

4.3. Na SOCIN, todos os colaboradores têm o dever de conhecer e cumprir estas diretrizes, como responsáveis pela preservação da confidencialidade, integridade e disponibilidade das informações, e somente sendo permitida a utilização das informações para fins internos. Todos devem preservar a imagem e a integridade das informações de clientes, colaboradores, prestadores de serviços e fornecedores, observando sempre o sigilo das informações.

4.4. A utilização de Internet, e-mail e mídias sociais por qualquer profissional que se relaciona com a SOCIN deve ser feita de forma responsável, ética e seguir as premissas de segurança da informação.

4.5. A informação corporativa pode se apresentar em diferentes formas, incluindo, mas não se limitando a: estratégia; conhecimento; indicador; estatística; projeto; pesquisa; ação de marketing; receita; prática; parecer; análise; experiência; inspeção; especificação; configuração; resultado.

4.6. A informação corporativa pode se apresentar em diferentes veículos, incluindo, mas não se limitando a: computadores; dispositivos de armazenamento; dispositivos móveis; caixas de e-mail; aplicativos de mensagens instantâneas; papel impresso ou manuscrito.

5. Atribuições

No contexto da presente PSI, destacam-se as seguintes atuações:

5.1. Responsável pela Segurança da Informação;
5.2. Gestores de cada departamento;
5.3. Equipe Técnica (inclusive terceiros);
5.4. Usuários;
5.5. Comitê Interno de Segurança da Informação e Proteção de Dados (Comitê SIPROD).

6. Princípios

Esta PSI se embasa nos seguintes princípios:

6.1. Confidencialidade: O acesso e manuseio de informações deve ser realizado apenas por pessoas que necessitam fazê-lo, mediante credenciais de acesso adequadas;
6.2. Integridade: As informações devem ser mantidas íntegras, consistentes e confiáveis, protegidas contra adulterações maliciosas ou acidentais;
6.3. Disponibilidade: As informações devem ser acessíveis no tempo e forma adequados para quem tiver as devidas credenciais de acesso;
6.4. Autenticidade e autenticação: Devem-se tomar medidas para que a identidade de quem produz (autenticidade) e acessa (autenticação) as informações sejam verificáveis;
6.5. Não-repúdio: Quando uma informação é transmitida, deve-se cuidar para que o processo de transmissão seja devidamente realizado, tanto do ponto de vista do remetente quanto do ponto de vista do destinatário.

7. Definições

Para os fins de interpretação desta PSI, consideram-se as definições a seguir listadas:

7.1. Responsável pela Segurança da Informação: pessoa física ou jurídica, contratada pela SOCIN para fazer a gestão das informações de uso desta;

7.2. Usuários: Funcionários ou Prestadores de Serviço terceirizados que tenham acesso regular ou eventual aos sistemas e informações de uso da SOCIN;

7.3. Ativos/serviços de informação: materiais, documentos, arquivos ou qualquer outro tipo de item, em qualquer formato, incluindo, mas não se limitando a, formatos digitais e físicos, que contenham qualquer tipo de informação;

7.4. Recursos computacionais: qualquer dispositivo eletrônico capaz de armazenar informação;

7.5. Áreas físicas: dependências imobiliárias da empresa;

7.6. Uso indevido: qualquer uso em desacordo com normas aplicáveis, incluindo, mas não se limitando a, quaisquer tipos de normas emitidas pelo Poder Público nas esferas Administrativa e Legislativa, bem como decisões judiciais e arbitrais, normas de órgãos de classe, cláusulas de contratos e acordos e normas internas da SOCIN ou de empresas terceiras que a SOCIN concordou em cumprir;

7.7. Incidentes de Segurança da Informação: quaisquer tipos de ocorrências que afetem ou tenham o potencial de afetar a confidencialidade, a integridade e a disponibilidade dos ativos/serviços de informação, recursos computacionais e áreas físicas da SOCIN, incluindo, mas não se limitando a, corrompimento de arquivos, avarias em dispositivos de armazenamento, acessos não autorizados, vazamentos e uso indevido;

7.8. Política de Segurança da Informação (PSI): é um conjunto de medidas e ações que visam a proteção dos pilares de segurança da informação e seus princípios, contra ameaças diversas, mitigando riscos e promovendo a continuidade das operações.

8. Regras e tarefas adotadas para proteger a segurança da informação

A presente PSI está estruturada com regras e tarefas que visam mitigar os riscos de vazamentos e perdas de informações em ambientes físicos e lógicos, conforme os itens a seguir.

8.1. USO DE SENHAS E CREDENCIAIS DE ACESSO

8.1.1. O Responsável pela Segurança da Informação da SOCIN deve gerenciar as credenciais de acesso a ativos/serviços de informação, recursos computacionais e áreas físicas desta, criando contas de acesso para seus usuários;

8.1.2. As senhas associadas às contas de acesso a ativos/serviços de informação, recursos computacionais e áreas físicas da SOCIN são de uso pessoal e intransferível, sendo dever e responsabilidade de cada usuário zelar por sua guarda e sigilo, sem prejuízo de sua responsabilidade por uso indevido por si ou por terceiros;

8.1.3. A autorização e o nível permitido de acesso a ativos/serviços de informação, recursos computacionais e áreas físicas da SOCIN é feita com base em perfis que definem o nível de acesso de cada usuário;

8.1.4. No caso de perda da credencial, o usuário deverá avisar imediatamente seu superior imediato e o Responsável pela Segurança da Informação e pela gestão das credenciais de acesso;

8.1.5. O uso indevido da credencial, seja intencional ou não, deverá ser comunicado ao superior imediato do usuário para que sejam tomadas as medidas administrativas e/ou legais cabíveis;

8.1.6. No caso de interrupção de vínculo do usuário com a SOCIN, o superior imediato deverá solicitar ao Responsável pela Segurança da Informação, a remoção dos acessos. A respectiva credencial de acesso deverá ser inativada de forma imediata pela área responsável e, consequentemente,

bloqueados os acessos aos ativos/serviços de informação ou recursos computacionais e áreas físicas da SOCIN;

8.1.7. A SOCIN poderá utilizar quaisquer ferramentas lícitas e idôneas para gestão de credenciais e controles de acesso aos seus ativos/serviços de informação ou recursos computacionais e suas áreas físicas.

8.2. PROTEÇÃO CONTRA AMEAÇAS E CÓDIGOS MALICIOSOS

8.2.1. A SOCIN utiliza ferramentas para operacionalizar medidas preventivas ou impeditivas para proteção, detecção e correção de ameaças e softwares maliciosos, tais como, mas não se limitando a, malwares e SPAM, que possam afetar seus ativos/serviços de informação, recursos computacionais e áreas físicas, incluindo, mas não se limitando a, estações de trabalho e dispositivos móveis;

8.2.2. Todos os arquivos recebidos por quaisquer meios, incluindo, mas não se limitando a, redes, mídias de armazenamento, e-mails, downloads e formulários em websites, deverão ser verificados quanto à presença de códigos maliciosos antes de serem abertos ou executados;

8.2.3. Para minimizar o risco de infecção por softwares maliciosos, os usuários devem usar, exclusivamente, softwares homologados, licenciados e instalados sob supervisão do Responsável pela Segurança da Informação da SOCIN;

8.2.4. O Responsável pela Segurança da Informação da SOCIN supervisionará a gestão, manutenção e atualização dos softwares de prevenção contra códigos maliciosos;

8.2.5. Mesmo com a existência de ferramentas para proteção contra códigos maliciosos, os usuários da SOCIN devem adotar um comportamento seguro, reduzindo a probabilidade de infecção ou propagação de softwares maliciosos.

8.3. ACESSO REMOTO

8.3.1. O acesso remoto aos ativos/serviços de informação e recursos computacionais da SOCIN é restrito a usuários que deles necessitem para execução das suas atividades profissionais;

8.3.2. O acesso remoto deverá ser monitorado, autorizado, transmitido por meio de VPN e protegido por criptografia e com autenticação através de senha de acesso;

8.3.3. As solicitações para acesso remoto, deverão ser formalizadas ao gestor de cada departamento, ao qual o colaborador está relacionado;

8.3.4. O usuário com acesso remoto autorizado, terá o mesmo perfil de acesso interno visualizando o mesmo ambiente de trabalho, respeitando o seu perfil de acesso aos ativos/serviços de informação e recursos computacionais da SOCIN;

8.3.5. Os usuários autorizados ao acesso remoto devem proteger suas credenciais observando as orientações no item “8.1” desta política (USO DE SENHAS E CREDENCIAIS DE ACESSO).

8.4. RESPOSTAS A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

8.4.1. Qualquer incidente de segurança da informação deverá ser registrado pelo Responsável pela Segurança da Informação;

8.4.2. O Responsável pela Segurança da Informação decidirá qual atitude tomar em relação a cada incidente ou a vários incidentes em conjunto, com base:

8.4.2.1. No Regimento Interno da Empresa;
8.4.2.2. Nesta PSI;
8.4.2.3. Em outras regras internas pertinentes; e
8.4.2.4. Na legislação aplicável.

8.4.3. Estão abrangidas nas possíveis atitudes em relação a incidentes de segurança da informação, entre outras:

8.4.3.1. A abordagem de incidentes como experiência para melhoria da segurança da informação;
8.4.3.2. A comunicação a órgãos públicos;
8.4.3.3. A comunicação aos clientes da SOCIN e ao público externo;
8.4.3.4. O uso como prova em processo judicial;
8.4.3.5. O uso como exemplo prático em capacitações e treinamentos.

8.4.4. O processo decisório sobre as atitudes que a SOCIN tomará a partir de incidentes de segurança da informação deve considerar como objetivos básicos os de minimizar qualquer tipo de impacto e recuperar as características de segurança da informação dos itens afetados;

8.4.5. Em quaisquer atitudes que a SOCIN tomar, a partir de incidentes de segurança da informação, deverão ser realizadas análises e procedimentos que resguardem a confidencialidade, incluindo o respeito a fatores como, entre outros, sigilo profissional, segredo industrial, segredo de justiça e proteção de dados pessoais;

8.4.6. Todos os incidentes de segurança da informação devem ser imediatamente comunicados ao Controlador de Tratamento de Dados Pessoais, para que este analise se o incidente afeta a proteção de dados pessoais e tome as medidas cabíveis, conforme a legislação aplicável.

8.5. USO ACEITÁVEL DOS ATIVOS DE INFORMAÇÃO

8.5.1. A SOCIN fornece, aos seus colaboradores, acesso aos ativos/serviços de informação, recursos computacionais e áreas físicas exclusivamente para o desempenho de suas atividades profissionais, salvo se de outra forma for disposto por escrito;

8.5.2. Os usuários devem estar atentos aos princípios de segurança da informação previstos nesta PSI, bem como o perfeito funcionamento na utilização dos ativos de tecnologia da informação;

8.5.3. Os usuários devem manter a integridade dos ativos físicos e de software, além de priorizar seu armazenamento em nuvem. Algumas mídias removíveis poderão ser utilizadas para execução dos trabalhos, conforme orientações do departamento responsável;

8.5.4. Os ativos/serviços de informação, recursos computacionais e áreas físicas devem ser inventariados, claramente identificados e registrados;

8.5.5. As instalações físicas para processamento de informações da SOCIN serão mantidas em áreas seguras, cujo perímetro é fisicamente isolado para evitar o acesso não autorizado, danos e quaisquer interferências de origem humana ou natural.

8.6. USO DE E-MAIL E ACESSO À INTERNET

8.6.1. A SOCIN contrata serviços de comunicação por e-mail e acesso à Internet para o uso de seus usuários autorizados exclusivamente para o desempenho de suas atividades profissionais;

8.6.2. Os serviços de comunicação por e-mail e de acesso à Internet contratados pela SOCIN devem ser continuamente monitorados por seu Responsável pela Segurança da Informação;

8.6.3. O monitoramento do serviço de comunicação por e-mail e de acesso à Internet contratados pela SOCIN tem como objetivos:

8.6.3.1. Proteger a SOCIN e seus colaboradores;

8.6.3.2. Atestar o respeito a esta PSI, ao Regimento Interno da SOCIN, e a outras regras aplicáveis;

8.6.3.3. Produzir evidências relativas à eventual violação desta PSI, do Regimento Interno da SOCIN, e de outras regras aplicáveis.

8.6.4. A publicação de conteúdos em mídias e redes sociais em nome da SOCIN é feita por departamentos e usuários que possuem essa responsabilidade específica, devendo os demais usuários evitar publicar qualquer tipo de informação em nome da SOCIN;

8.6.5. Não é permitida a publicação de qualquer tipo de material, incluindo, mas não se limitando a, imagens, fotos, vídeos e áudios relacionados ao ambiente corporativo físico ou digital da SOCIN sem a expressa autorização de seus dirigentes;

8.6.6. Os itens previstos neste tópico devem ser compreendidos em consonância com as proibições previstas no Regimento Interno da SOCIN, item I.2.2 (Das proibições específicas – utilização da internet e redes de dados), bem como com o disposto no item VIII (Do relacionamento interpessoal dentro da empresa) e item X.2 (Do uso da Internet) do mencionado Regimento Interno.

8.7. USO E CONTROLE DE CRIPTOGRAFIA

8.7.1. A SOCIN deverá utilizar controle de criptografia para promover a segurança das informações que são trafegadas ou armazenadas em seus ativos de informação;

8.7.2. Assinaturas digitais poderão ser utilizadas para validar a autenticidade ou integridade de informações armazenadas ou transmitidas;

8.7.3. Dados em trânsito nos sites e servidores em nuvem devem ser protegidos através do protocolo HTTPS, com certificado criptografado 256bits;

8.7.4. O tráfego de login/senha de rede, durante a autenticação de usuários, e de informações, nos sistemas ou serviços disponibilizados pela SOCIN, deve ser protegido com o uso de mecanismos de criptografia como HTTPS, SSL, TLS e VPN.

8.8. CAPACITAÇÃO E CONSCIENTIZAÇÃO

8.8.1. A SOCIN considera fundamental a capacitação e a conscientização de seus colaboradores sobre tópicos referentes à segurança da informação, incluindo, mas não se limitando a, tópicos sobre princípios da segurança da informação, prevenção, gerenciamento de riscos e proteção de dados;

8.8.2. A SOCIN promoverá o aprendizado contínuo, usando de recursos educacionais ou instrucionais para tal finalidade;

8.8.3. Os colaboradores da SOCIN deverão ser capacitados para a utilização dos ativos/serviços de informação, recursos computacionais e áreas físicas da SOCIN e para a aplicação dos conceitos e princípios de segurança da informação, de forma a promover níveis adequados de confidencialidade, integridade e disponibilidade das informações e proteção de dados pessoais;

8.8.4. Todos os colaboradores da SOCIN devem ser incentivados a valorizar a capacitação e a conscientização sobre tópicos referentes à segurança da informação, promovendo o conhecimento, enquanto importante elemento de desenvolvimento dela e deles próprios;

8.8.5. A SOCIN incentiva e valoriza a sinceridade intelectual, devendo esta ser entendida como a conduta ética de não fazer mais do que esteja ao alcance das competências e habilidades atuais. Além disso, a SOCIN incentiva a manifestação de dúvidas sempre que existirem, a fim de promover a melhoria contínua do processo de ensino-aprendizagem sobre tópicos referentes à segurança da informação.

8.9. CRONOGRAMA DE BACKUP

A SOCIN deve manter cronogramas de backup adequados aos princípios e regras previstos na presente PSI. A SOCIN considera seus procedimentos de backup como

informação sensível, portanto procedimentos referentes a backup devem ser previstos em documento confidencial complementar a esta PSI.

8.10. PLANO DE CONTINGÊNCIA

Os ativos de informação da SOCIN estão preponderantemente armazenados em servidores hospedados em *data centers* dos diversos sistemas de gestão contratados pela SOCIN. São, preferencialmente, sistemas de empresas de grande porte, internacionalmente renomadas e reconhecidas pela segurança e disponibilidade oferecida de seus serviços. A SOCIN considera seu plano de contingência como sendo informação sensível, portanto informações referentes a plano de contingência, incluindo, mas não se limitando, aos serviços contratados pela SOCIN e respectivos níveis de serviço devem ser descritos em documento confidencial complementar a esta PSI.

8.11. TRATAMENTO DE DADOS PESSOAIS

8.11.1. A SOCIN valoriza a proteção de dados pessoais e a conformidade com as normas sobre proteção de dados pessoais;

8.11.2. A SOCIN considera a proteção de dados pessoais a partir de princípios legais, materializando-os a partir de uma política de tratamento de dados e privacidade e atitudes correspondentes baseadas em decisões do Controlador do Tratamento de Dados Pessoais.

8.12. TRATATIVA DOS DADOS EM AMBIENTES DE TESTES E PRODUÇÃO

8.12.1. A SOCIN possui uma metodologia de desenvolvimento e manutenção de sistemas de informação que deve ser seguida observando-se suas formalidades, necessidades de documentação de software e utilizações de ferramentas de gestão;

8.12.2. Antes de disponibilizar nova versão de uma aplicação para o ambiente de produção dos Clientes da SOCIN, o usuário deve realizar os testes e validações internas;

8.12.3. Com o objetivo de minimizar os riscos e restringir acessos indevidos, o ambiente de produção deve ser acessado apenas por usuários que têm autorização do gestor do departamento;

8.12.4. A atualização dos códigos-fonte deve ser efetuada apenas após autorização formal, seguindo procedimentos de controle de mudança e versão;

8.12.5. Para promover a continuidade e a segurança, e evitar mudanças não registradas e autorizadas em sistemas de informação, todo acesso aos códigos-fonte deve ser restrito e controlado;

8.12.6. O acesso aos ambientes de desenvolvimento, teste e produção será restrito apenas aos perfis definidos pela SOCIN;

8.12.7. As bases de dados dos ambientes de produção, testes e desenvolvimento devem ser utilizadas especificamente para suas respectivas funcionalidades, não sendo permitida a utilização de uma base de dados para funcionalidades diferentes da especificada.

9. DISPOSIÇÕES FINAIS

A SOCIN reafirma a importância da implementação e manutenção da segurança de quaisquer tipos de ativos de informação necessários para o desenvolvimento de suas atividades empresariais. Nesse sentido, a SOCIN buscará adotar sempre as melhores práticas em segurança da informação.