POLÍTICA DE SEGURANÇA CIBERNÉTICA E DA INFORMAÇÃO TRAUTE PAY

1. APRESENTAÇÃO

A Política de Segurança Cibernética e da Informação é o documento que estabelece conceitos, diretrizes e responsabilidades sobre os principais aspectos relacionados à segurança cibernética e segurança da informação, visando preservar a confidencialidade, integridade, disponibilidade e conformidade de todas as informações sob gestão do **TRAUTE PAY**.

Busca também, definir os princípios fundamentais que formam a base da Política de Segurança Cibernética e da Informação, norteando a elaboração de normas, processos, padrões e procedimentos, conforme as previsões regulatórias. Com isso, objetivando a proteção dos seus parceiros, colaboradores e a própria empresa da utilização indevida desses dados que possam comprometer o TRAUTE PAY em seus serviços de rede e sistemas, bem como suas situações reputacionais.

2. ABRANGÊNCIA

A Política de Segurança Cibernética e da Informação tem abrangência corporativa do **TRAUTE PAY**, ou seja, afeta todas as suas áreas de negócio, escritórios e demais operações no que se refere à ocorrência de incidentes de segurança da informação.

3. CONCEITOS E DEFINIÇÕES

●Recursos
Qualquer ativo, tangível ou intangível, pertencentes, a serviço ou sob responsabilidade do TRAUTE PAY, que possua valor para a empresa. Podem ser considerados recursos: pessoas, ambientes físicos, tecnologias, serviços contratados, em nuvem, sistemas e processos.

●Ameaça
Qualquer causa potencial de um incidente indesejado que possa resultar em impacto nos objetivos do negócio. As ameaças podem ser internas ou externas, intencionais ou não intencionais.

●Controle
Qualquer recurso ou medida que assegure formas de tratamento de riscos, incluindo a redução, eliminação ou transferência. A implantação e manutenção adequada de controles materializa a segurança das informações.
Podem ser interpretados como controles: políticas, processos, estruturas organizacionais, técnicas padrões, software, hardware e outros.

●Gestor
Colaborador que exerce cargo de liderança, como: Diretor Presidente, Coordenador, Supervisores de seção.

●Informação
Qualquer conjunto organizado de dados que possua algum propósito e valor para o sistema do TRAUTE PAY, seus clientes, parceiros e colaboradores. A informação pode ser de propriedade da empresa, estar sob sua custódia ou sob custódia de terceiros, como exemplo, informações armazenadas em nuvem.

●Princípios de “least privilege” i "need to know”
Estes princípios devem reger a autorização de qualquer acesso a sistemas e informações. Segundo eles, deve ser concedido apenas o nível mínimo de acesso (Least Privilege) a quem realmente tenha a necessidade de acesso (Need to Know).

●Política de Segurança Cibernética e da Informação

Estrutura de documentos formada pela política, normas e padrões de segurança cibernética e segurança da informação.

●Segurança da Informação (SI)
É a proteção das informações, sendo caracterizada pela preservação de:

I. Confidencialidade: garantia de que a informação somente será acessada por pessoas efetivamente autorizadas;

II. Integridade: garantia de que o conteúdo da mensagem não será alterado ou violado indevidamente, ou seja, mede a exatidão da informação e seus métodos de modificação, manutenção e validade.
III. Disponibilidade: garantia de que os Colaboradores autorizados obtenham acesso à informação e aos sistemas correspondentes sempre que necessários, nos períodos e ambientes aprovados pela empresa;
IV. Conformidade: garantia de que controles de segurança da informação, devidamente estabelecidos, estão sendo executados conforme esperado e produzindo resultados efetivos no cumprimento de seus objetivos.

●Segurança Cibernética
Conjunto de tecnologias, processos e práticas projetados para proteger redes, computadores, sistemas e dados de ataques, danos ou acesso não autorizado. Também conhecida como Segurança de TI, visa proteger somente assuntos relacionados ao digital.

●Recursos Críticos

Recursos essenciais para o funcionamento da operação do sistema da **TRAUTE PAY** e que possuem informações críticas ou sensíveis.

4. DIRETRIZES

A informação é um ativo essencial para os negócios do **TRAUTE PAY**, e, sendo assim, deve ser adequadamente protegida.
A segurança cibernética e da informação visa proteger as informações contra diversos tipos de ameaças, para minimizar a exposição da empresa a riscos, garantindo que as características fundamentais da informação sejam preservadas, sendo elas: confidencialidade, integridade, disponibilidade e conformidade.
O **TRAUTE PAY** está alinhado com os objetivos e requisitos do negócio, estabelece nesta Política de Segurança Cibernética e da Informação, regras e direcionamentos a serem seguidos e aplicados a pessoas, processos e tecnologia, de forma a proteger as informações do **TRAUTE PAY**, de seus clientes, fornecedores e parceiros de negócios.
Seguir as diretrizes desta política, significa proteger a empresa contra o vazamento de informações, contra fraudes, zelar pela privacidade, garantir que sistemas e informações estejam disponíveis quando necessário e zelar pela proteção da imagem e das marcas **TRAUTE PAY**.

5. PAPÉIS E RESPONSABILIDADES

Todo colaborador, independente do cargo, função ou local de trabalho, é responsável pela segurança das informações do **TRAUTE PAY** e deve cumprir as determinações da política, normas e padrões de segurança da informação.

5.1 O NÃO CUMPRIMENTO DESSA POLÍTICA

O não cumprimento desta Política acarretará sanções administrativas, podendo acarretar o desligamento do colaborador ou rescisão do contrato vigente e a reparação de danos, de acordo com a gravidade da ocorrência.

6. DIRETRIZES PARA TRATAMENTO DAS INFORMAÇÕES

Toda informação deve ter regras claramente definidas pelo seu proprietário para proteção contra perda, alteração e acesso, seja ela armazenada em meio eletrônico (computador central, servidores de rede, microcomputadores, pen drive), em papel (correspondências, atas, relatórios, manuscritos etc.) ou outros meios.
Toda informação deve ter usuários explicitamente definidos (instituições, áreas, pessoas) e os tipos de direitos que cada um terá para acessá-la.
Toda informação deverá ter procedimentos para protegê-la do acesso de pessoas não autorizadas.
Toda informação que garanta a continuidade das atividades dos integrantes do **TRAUTE PAY**, deverá ter cópia de segurança em local físico distinto, devidamente protegido para essa finalidade ou outro meio eficiente para permitir sua pronta recuperação em caso de perda ou danos.
As informações contidas em material que se tornar disponível para descarte (papel, pendrives, cd etc.) deverão ser destruídas ou mantidas em locais fechados, protegidos do acesso de pessoas não autorizadas.
Todo colaborador do TRAUTE PAY é responsável pela segurança da informação a que tem acesso.

Toda informação encontrada extraviada deverá ser, imediatamente, devolvida à sua origem.

7. RECOMENDAÇÕES PARA O TRATAMENTO DA INFORMAÇÃO

Os colaboradores não devem efetuar tentativas de obter acesso às informações que não lhe são permitidas, devendo solicitá-las ao respectivo proprietário da informação, pasta ou arquivo.
A elaboração das normas e procedimentos de acesso deverá levar em consideração os riscos do acesso e alteração não autorizados, divulgação indevida e indisponibilidade dos dados, que tem por consequência às fraudes, problemas legais, perdas de negócios, danos à imagem e dificuldade na recuperação da informação.

8. OBJETIVO E DIRETRIZES PARA CLASSIFICAÇÃO DA INFORMAÇÃO

A classificação da Informação tem o objetivo de proporcionar ao usuário a possibilidade de analisar suas informações, facilitando a definição do seu nível de acesso e condições de armazenamento, considerando sua confidencialidade, integridade e disponibilidade.
Todas as informações devem ser classificadas.
Toda a informação deverá ser considerada sigilosa e de alto risco até que se tenha estabelecido sua classificação.
A proteção proporcionada à informação, tanto em termos de acesso quanto de conservação, deve estar de acordo com sua classificação.
Quando em um mesmo meio físico existirem informações classificadas de formas diferentes, deve-se adotar, para fins de segurança, a classificação mais restrita.
Sempre que forem efetuadas alterações significativas em um sistema informatizado, ou nas características de uma informação, deverá ser comunicado aos usuários com antecedência e efetuada uma revisão de classificação.

9. CONCEITOS DE CONFIDENCIALIDADE

Os tipos de informações podem ser:
I. Informações Sigilosas: Informações extremamente restritas quanto a sua divulgação. São de alto valor por motivos estratégicos e/ou com a possibilidade de provocar prejuízos, razão pela qual seu nível de proteção deve ser o mais alto possível;
II. Informações Confidenciais: Informações de caráter setorial e para divulgação a um reduzido grupo de pessoas de uma área ou setor de atividade;

III. Informações Internas: São aquelas utilizadas no âmbito interno da organização, sobre questões que venham a ser importantes para os colaboradores.
IV. Informações Públicas: São aquelas que circulam livremente, interna e externamente, em relação ao TRAUTE PAY, não havendo interesse em controlar sua divulgação e acesso.

10. CONCEITOS DE INTEGRIDADE E DISPONIBILIDADE

Os tipos de informações podem ser:
I. De Alto Risco: Informações cuja indisponibilidade e/ou inexatidão poderão causar prejuízos à continuidade dos negócios.
II. De Médio Risco: Informações que impõem ao negócio problemas de disponibilidade e dificuldade na recuperação. O proprietário da informação e os usuários aceitam a disponibilidade limitada e a existência de um determinado tempo para recuperação.
III. De Baixo Risco: Informações cuja exatidão e acessibilidade apresentam pouco ou nenhum risco ao negócio. Os usuários aceitam eventuais indisponibilidades e longos períodos para recuperação das informações.

11. ADMINISTRAÇÃO DE ACESSO DE USUÁRIOS

A área responsável pelo controle de acesso aos sistemas deverá manter procedimentos formais que contemplem desde o registro inicial para um novo usuário à administração de privilégios e senhas e o cancelamento de autorizações.
A área responsável pelo controle de acesso deverá prover a prevenção de acessos não autorizados.

Cada usuário deverá gravar os arquivos de sua competência em pasta própria, ficando assim, responsável pelo conteúdo de sua pasta.
O controle de acesso deverá assegurar que os usuários de computadores, conectados à rede corporativa do **TRAUTE PAY**, não comprometam a segurança de qualquer sistema operacional ou produto. Para isso, toda singular do sistema deverá possuir um servidor de controlador de domínio que garanta que o usuário não efetue alterações indevidas na estação de trabalho. Além disso, todos os computadores/notebooks devem estar com antivírus corporativo devidamente instalados.
A área responsável pelo controle de acesso deverá prover a prevenção de

acessos não autorizados.
A inserção de qualquer nova informação, realizada por meio de dispositivos removíveis só será liberada mediante autorização do gerente ou gestor do setor responsável. Antes de efetuar a liberação, deverá ser verificado se a estação de trabalho realmente possui antivírus instalado e atualizado.
O acesso a serviços computacionais deverá sempre ocorrer através de um procedimento seguro no qual o usuário conecta-se a um sistema de controle utilizando seu usuário e senha, devendo ser planejado para minimizar os riscos de acesso não autorizados.
O acesso às estações de trabalho de forma remota só deverá ocorrer mediante autorização do usuário da estação de trabalho.

12. ASPECTOS GERAIS DA SEGURANÇA FÍSICA DE COMPUTADORES E DE SERVIDORES

A estrutura para manter a segurança física dos equipamentos de rede e computadores, devem obedecer aos padrões de segurança gerais e adequar- se, no mínimo, às especificações dispostas neste item.
As dimensões do local devem ser suficientes para a instalação dos equipamentos de rede e microcomputadores. Bem como as entradas de ar (ventilação) dos equipamentos devem estar desobstruídas.
A disposição dos cabos lógicos e de energia devem ser instalados em canaletas específicas para que não haja interferência na rede e deve ser adequada para que as pessoas possam transitar livremente.

13. PLANO DE RETENÇÃO DE DADOS

O **TRAUTE PAY** deverá manter políticas de Retenção de Dados, considerando as normas aplicáveis, relacionadas aos dados pessoais.

14. CONSCIENTIZAÇÃO E DIVULGAÇÃO DA SEGURANÇA CIBERNÉTICA E DA INFORMAÇÃO

Os recursos e as informações de propriedade ou sob custódia do **TRAUTE PAY** devem ser utilizados de acordo com os interesses da organização, para prestação dos seus serviços, atendendo aos requisitos e respeitando as regras estabelecidas.

A política de segurança cibernética e da informação, normas e padrões de segurança devem ser amplamente divulgadas no processo de admissão e integração de novos colaboradores, tanto pelas equipes de recursos humanos quanto pelos gestores.
Programas de conscientização, divulgação e reciclagem do conhecimento da política de segurança cibernética e da Informação devem ser estabelecidos e praticados regularmente para garantir que todos os colaboradores e terceiros conheçam as diretrizes e responsabilidades relacionadas à segurança das informações.

15. INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

São considerados incidentes de segurança da informação quaisquer eventos adversos de segurança, confirmados ou sob suspeita, que levem ou possam levar ao comprometimento de um ou mais dos princípios básicos de SI: confidencialidade, integridade, disponibilidade e conformidade, colocando o negócio em risco.
Violações ou tentativas de violação desta política, de normas ou de controles de segurança da informação, intencionais ou não, são considerados incidentes de segurança.

16. PREVENÇÃO E DETECÇÃO DE INTRUSÃO

Todos os recursos do sistema de informação expostos à Internet devem ser acompanhados e protegidos por um IDS / IPS.

Sempre que o IDS / IPS detecta ou responde a uma tentativa externa mal-intencionada suficientemente grave para ameaçar os recursos do sistema de informações protegidas, uma análise estruturada e procedimento de resposta deve ser acionado.

17. PLANO DE RESPOSTA A INCIDENTES

O **TRAUTE PAY** deverá elaborar cenários de incidentes, durante os testes de continuidade de negócios, com o objetivo de identificar eventos que possam dificultar a operação e promover queda no desempenho, obstrução ou erro na execução de processos organizacionais que impossibilitam a regular operação dos serviços.

Nos casos de incidentes, o Terceiro ou Colaborador tem o dever de notificar o Departamento de Tecnologia do TRAUTE PAY, o mais rápido possível, para que sejam tomadas as medidas de segurança.

18. PROTEÇÃO CONTRA CÓDIGOS MALICIOSOS

Deverão ser implementados controles tecnológicos para a proteção dos equipamentos de processamento de informação que executem algum tipo de software (tanto de usuário final como servidores) para a prevenção, detecção, correção e erradicação de códigos executáveis maliciosos.

19. AUDITORIA

O **TRAUTE PAY** se reserva o direito de auditar qualquer dispositivo utilizado pelos indivíduos sujeitos a esta Política durante o desempenho das atividades comerciais ou funções, para este fim serão solicitados os acessos, que podem incluir (rol exemplificativo):

- Nível de usuário e/ou acesso em nível de sistema a qualquer computação ou comunicação;
- Acesso às informações (eletrônicas, impressas, etc.) que possam ser produzidas, transmitidas ou armazenadas em equipamentos ou instalações do **TRAUTE PAY**;
- Acesso às áreas de trabalho (escritórios, cubículos, áreas de armazenamento, data centers, centros de operações, etc.);
- Acesso para monitorar e registrar interativamente o tráfego nas redes do **TRAUTE PAY**.

Esta auditoria deve observar as regras da Lei Geral de Proteção de Dados e sua possibilidade informada na Comunicação Interna de Privacidade aos colaboradores do **TRAUTE PAY**

20. ATUALIZAÇÃO DA POLÍTICA

A atualização da presente Política ocorrerá sempre que alterações legislativas ou regulatórias relevantes ocorrerem, sendo de responsabilidade da Alta Administração ou do setor de compliance, realizar as alterações e submetê-la à aprovação da Alta Administração.

21. VIGÊNCIA

A presente Política foi aprovada pelos membros componentes da Alta Administração, entrando em vigência na data da sua aprovação.
A vigência desta Política é indeterminada, podendo ser substituída apenas por uma versão atualizada.