RESUMO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO CIBERNÉTICA

1. Introdução

Em conformidade com a Resolução nº 4.658/18a B&T Corretora elaborou a Política de Segurança da Informação Cibernética instituindo diretrizes de forma a assegurar a confidencialidade, integridade e disponibilidade dos dados de sua propriedade e/ou sob sua guarda e dos sistemas de informações utilizados.

2. Objetivos

O objetivo da Política de Segurança da Informação Cibernética é estabelecer os padrões e regras necessárias para a elaboração dos controles e dos documentos referentes a Segurança da Informação da B&T Corretora, assegurar a continuidade do negócio e minimizar danos causados pelo impacto de incidentes de segurança, além de proteger os ativos de Informação da B&T e seus respectivos clientes.

3. Escopo

Esta política é mandatória para a segurança dos processos de negócio interno e externos da **B&T CORRETORA**.

A política também é destinada a todas as formas intelectuais e físicas de ativos da informação tanto próprios, como usados ou mantidos em custódia pela **B&T**. Estas formas incluem *hardware*, redes, *software* e dados, tanto armazenados e processados em computadores, transmitidos através de redes, impressos ou escritos, enviados por fax, armazenados em mídias removíveis ou falados em conversas e ligações telefônicas ou postadas na Internet ou assemelhados.

Para Permitir uma abordagem estruturada para a segurança da informação foi definida uma arquitetura em camadas, que consiste nos seguintes elementos:

- Política de Segurança da Informação Cibernética;

- Controles de Segurança de Informações;
- Normas, Procedimentos e Diretrizes de Segurança da Informação;

4. Princípios da Segurança da Informação Cibernética

São princípios da Segurança da Informação Cibernética a:

- **Confidencialidade**: A informação não é disponibilizada ou divulgada a Indivíduos, entidades, ou processos não autorizados.
- **Integridade**: Dados não são alterados ou destruídos de forma não autorizada. O sistema executa a sua função da maneira prevista, sem que haja manipulações deliberadas ou acidentais não autorizadas.
- **Disponibilidade**: Ativos que são acessíveis a partes autorizadas nos momentos apropriados.
- **Autenticidade**: É um processo que se estabelece a validade
- **Legalidade**: A informação é armazenada, transmitida, acessada e retirada de acordo com os termos legais existentes.
- **Não repúdio**: São as partes envolvidas em uma transação que as capazes de provar posteriormente, o que aconteceu.

5. Diretrizes Gerais da Política de Segurança da Informação Cibernéticas.

A presente Política estabelece diretrizes de forma a assegurar que:

- As informações serão protegidas contra acesso não-autorizado;
- A confidencialidade das informações será assegurada;
- A Integridade das informações será mantida;
- Requisitos do negócio quanto à disponibilidade da informação e sistemas serão atendidos;
- A Gestão de Risco será executada para identificar e avaliar riscos de segurança para que medidas apropriadas possam ser adotadas;
- A classificação de ativos de informação será aplicada;
- Requisitos legais e regulatórios do país, bem como requisitos contratuais de segurança, serão atendidos;

- Treinamento em Segurança de Informações é mandatório para todos os colaboradores;
- Padrões, procedimentos e diretrizes adicionais deverão ser elaborados localmente para apoiar a implementação da política global de acordo com a legislação local. Estas regras definem o nível mínimo de conformidade para todos os funcionários sobre Segurança da Informação;
- Todos os gestores são diretamente responsáveis pela Implementação da Política dentro de suas áreas de negócio e pela adesão a mesma pelas suas equipes;
- É responsabilidade de cada funcionário aderir à Política de Segurança da Informação e aos padrões, procedimentos e diretrizes relacionados. Violações podem resultar em ações disciplinares, até e inclusive demissão;
- Todos os colaboradores **devem** reportar violações de Segurança de Informações, reais ou potenciais, ao seu gestor ou ao *gestor de T.I*. No caso de um incidente de segurança ações imediatas devem ser tomadas para reduzir os riscos e impactos de danos para a B&T e nossos clientes;
- Exceções a esta Política de Segurança da Informação requerem aprovação do Departamento de Tecnologia da Informação;
- Nesse contexto, os domínios de segurança lógica e segurança física (pessoas e sites) contribuem para reforçar a proteção das informações.

6. Normas

- **Norma de Gestão de Ativos -** Esta norma traz a divulgação das diretrizes de proteção dos ativos da organização por meio do estabelecimento e manutenção de inventários e definição de proprietários a estes ativos, visando a manutenção de informações sobre a eficácia dos controles de segurança, assegurando a proteção adequada.
- **Norma de Segurança em Recursos Humanos -** Proteger os ativos, incluindo a informação da **B&T** através da realização segura de admissões, demissões e mudanças de cargo, além da promoção da conscientização da Política de Segurança da Informação, assegurando que todos os colaboradores incluídos no âmbito da empresa entendam claramente suas responsabilidades, através do **Código de Ética e Conduta** concordando com as regras previstas na política vigente.
- **Norma de Segurança Física e do Ambiente -** Define as diretrizes para a proteção dos ambientes físicos da **B&T**, minimizando os riscos para as instalações onde informações

críticas e confidenciais são geradas, processadas ou mantidas e elevando a proteção dos ativos físicos, em conformidade com os riscos identificados.

- **Norma de Gestão das Operações e Comunicações -** Visa proteger todas as operações relacionadas ao manuseio de mídias, troca de informações, internet, correio eletrônico, transferência de arquivos e utilização da rede da **B&T** respeitando a classificação do sigilo das informações em questão.
- **Norma de Controle de Acesso Lógico -** É definida a partir da adoção de dois processos básicos: identificação e autenticação (quem está acessando) e autorização (quais os privilégios deste usuário no sistema e o que se pode acessar).
- **Norma de Aquisição, Desenvolvimento e Manutenção de Sistemas da Informação -** Visa **e**fetivar e garantir que a segurança seja parte integrante em todo o âmbito de sistemas da informação da **B&T**, estabelecendo padrões de segurança na aquisição, no desenvolvimento e manutenção de sistemas da informação.
- **Norma de Tratamento de Incidente em Segurança da Informação -** Discorre sobre como comunicar os incidentes ocorridos no âmbito de segurança da **B&T** permitindo a tomada de ação para correção no menor tempo possível. Tais incidentes podem ser violação de acesso, mau funcionamento dos sistemas, perdas ou danos de equipamentos e recursos computacionais, não conformidade com as políticas de informação vigentes ou até mesmo erros humanos, acidentais ou incidentais.
- **Norma de Continuidade de Negócios -** Define as diretrizes que visam identificar e reduzir os impactos em consequência de desastres, falhas de segurança, perdas de serviços e disponibilidade de negócios, limitando a consequência dos danos do incidente, garantindo que os ativos de informações requeridas aos processos de negócios da **B&T** estejam prontamente disponíveis.
- **Norma de Conformidade em Segurança da Informação -** Visa padronizar a conduta interna na **B&T** no que diz respeito aos seus recursos computacionais, processos e recursos humanos, minimizando ameaças e combatendo-as através da aplicação de controles em segurança da informação.
- **Norma de Segurança do Acesso de Usuários -** O acesso de usuários aos sistemas é concedido com base no princípio da necessidade da informações para a execução da função do colaborador, nesse sentido a presente norma descreve todos os procedimentos e obrigações dos usuários para a realização do acesso seguro a sistemas e redes da empresa, assim como de clientes e parceiros que tenham necessidade de direitos de acesso.

- **Norma de Segurança de Rede -** Visa garantir que medidas de segurança adequadas sejam tomadas quanto a todos os serviços de rede da empresa, assim como sua classificação e direitos de acesso pelos usuários, além de estabelecer regulamentos para sistemas de comunicação eficazes e seguros.
- **Norma de Segurança em Correio Eletrônico -** Nesta norma estão definidas as diretrizes que devem ser observadas na utilização de correio eletrônico dentro da **B&T**. Por sistema de correio eletrônico entendem-se sistemas, programas, servidores que se utilizam do protocolo SMTP, IMAP e POP para o envio de mensagens, englobando desde o *software* cliente do usuário até HTTP/HTTPS a servidores de correio eletrônico.
- **Norma de Segurança da Internet -** Esta norma define os padrões para a o uso seguro da Internet em todo o âmbito da **B&T**, estabelecendo padrões e regras para seus colaboradores, terceiros, parceiros e clientes.
- **Norma de Acesso à Rede Privada -** Descreve as diretrizes gerais e obrigações dos usuários para o uso apropriado de conexões às redes privadas (VPN) da **B&T**, assim como de clientes e parceiros que tenham necessidade de acesso, visando prover mais segurança e desempenho neste processo.
- **Norma de Segurança de Acesso Físico -** Descreve as diretrizes gerais para o estabelecimento de um sistema efetivo de identificação de pessoas (colaboradores, visitantes e prestadores de serviço), manutenção do controle da movimentação desta pessoa dentro da organização e que possa ser facilmente identificado por todos, e principalmente pelos colaboradores do **Departamento de Tecnologia da Informação** da **B&T**, visando aumentar a segurança física geral da organização.
- **Norma de Tratamento de Dados -** Este documento define as diretrizes para a proteção de dados dentro e fora do ambiente da **B&T**, visando identificar e reduzir os impactos em casos de vazamento de dados ou uso indevido das informações pessoais confidenciais e corporativas por parte de seus funcionários e colaboradores. Esta norma igualmente abrange as diretrizes para uso, pela **B&T**, das informações pessoais de seus funcionários e colaboradores

A **B&T Corretora de Câmbio** declara que o exposto se refere ao resumo da **Política de Segurança da Informação Cibernética** vigente a qual está sob responsabilidade do departamento de **Tecnologia da Informação** e foi divulgada a todos os seus colaboradores, parceiros, terceirizados e prestadores de serviços.