Sttórico sistemas

Política de Segurança da Informação

1. Introdução

1.1. Consideramos a Segurança da informação como parte integrante do ciclo de vida dos processos de negócios da empresa, por isso esta Política é uma declaração formal da Sttórico Sistemas (STT) sobre seu compromisso com a proteção da informação, devendo ser cumprida por todos os usuários das informações de sua propriedade e/ou sob sua guarda.

2. Objetivo

2.1. A Política de Segurança da Informação (PSI) tem como objetivo definir a direção, os princípios e as regras básicas de gestão da segurança da informação, visando garantir a confidencialidade, integridade e a disponibilidade da informação de sua propriedade e/ou sob sua guarda em conformidade com as disposições constitucionais, legais e regimentais vigentes.

3. Abrangência

3.1. A PSI é um normativo interno com valor jurídico e aplicabilidade imediata, restrita a todos os ativos tangíveis ou intangíveis da STT, seja em ambiente físico ou lógico, compreendendo as seguintes áreas da empresa: Direção da Empresa; Segurança da Informação; Infraestrutura; Recursos Humanos; Governança de TI; Controles Internos e Riscos Operacionais.

4. Documentos de Referência

- ABNT NBR ISO/IEC 27001:2013
- Lista de obrigações Legais, Regulamentares e Contratuais
- Plano de negócios da STT

5. Princípios Básicos de Segurança da Informação

As ações de segurança da informação serão norteadas pelos seguintes princípios:

- **Confidencialidade** – Garantir o acesso às informações somente para pessoas autorizadas ou sistemas habilitados;
- **Integridade** – Garantir a exatidão da informação;
- **Disponibilidade** – Garantir que a informação esteja sempre disponível;
- **Celeridade**: Garantir respostas rápidas a incidentes e falhas de segurança;
- **Ética**: Garantir os direitos e interesses legítimos dos usuários e dos nossos clientes;
- **Clareza**: Garantir que as regras de segurança dos ativos de segurança da informação e comunicações sejam precisas, concisas e de fácil entendimento;
- **Legalidade**: Garantir a conformidade das ações de segurança com as atribuições regimentais e legais;
- **Publicidade**: Garantir que o manuseio da informação seja transparente, observando os critérios legais.

6. Diretrizes Gerais de Segurança da Informação

6.1. Todo dado ou conteúdo escrito, verbal ou apresentado de modo tangível ou intangível, que tenha valor pessoal ou para a empresa, deve ser considerado informação sigilosa, sendo utilizada com cautela e apenas por pessoas autorizadas.

6.2. Deve ser preservado os critérios de confidencialidade, integridade e disponibilidade da informação.

6.3. Deve ser protegido e preservado os recursos institucionais, a marca, a reputação, o conhecimento e a propriedade intelectual da empresa.

6.4. Todos os ativos tangíveis e intangíveis da empresa devem receber proteção contra roubo, fraude, espionagem, perda não-intencional, acidentes e outras ameaças.

6.5. Os princípios e as regras da Segurança da Informação devem ser disseminamos a todos os usuários, funcionários, colaboradores e prestadores de serviços da empresa.

6.6. Todo acesso às informações e aos ambientes lógicos deve ser controlado.

6.7. As autorizações de acesso às informações e aos ambientes lógicos devem ser realizadas por meio do uso de identidade digital (*login e senha*) pessoal e intransferível, revistas, confirmadas e registradas continuadamente de forma a garantir acesso as informações apenas às pessoas devidamente autorizadas.

6.8. Todo manuseio, tratamento, controle e proteção dos dados e informações de propriedade e/ou sob guarda da empresa deve ser realizado de forma adequada e com responsabilidade.

7. Diretrizes de Confidencialidade

7.1. Deve ser garantido o acesso às informações somente para pessoas autorizadas ou sistemas habilitados.

7.2. Toda informação que envolve os dados pessoais, financeiros, comerciais, estratégicos, técnicas e Know-how da empresa ou sob sua guarda, sejam elas na forma de modelos, diagramas, planos, extratos, relatórios ou em códigos de programação deve ser tratada como confidencial.

7.3. Deve ser estabelecido critérios de confidencialidade e classificação da informação, e determinado o nível da segurança requerida para garantir seu manuseio ou acesso somente por pessoa autorizada.

7.4. O sigilo pessoal, profissional e contratual deve ser respeitado, quaisquer informações classificadas como confidenciais não podem ser reveladas, transferidas, compartilhadas ou divulgadas sem a devida autorização

7.5. Os testes de desenvolvimento de sistemas devem utilizar dados fictícios, preservando a privacidade e segurança dos dados e informações confidenciais.

8. Diretrizes de Integridade

8.1. Deve ser garantida a exatidão da informação.

8.2. Toda informação deve ser armazenada em local apropriado e protegida contra acesso, modificação, destruição ou divulgação não autorizados.

8.3. Todas as informações em meio físico devem ser guardadas em gavetas, armários trancados ou em local apropriado e seguro quando não estão sendo utilizadas.

8.4. Deve ser estabelecido os espaços físicos e lógicos seguros para proteger as áreas que criam, desenvolvem, processam ou armazenam informações críticas e que contenham ativos críticos para a empresa.

8.5. Para asseguramos a contínua integridade das informações, deve ser mantida uma correta manutenção dos ativos críticos da empresa, mantendo-os protegidos contra a falta de energia elétrica e outras interrupções causadas por possíveis falhas.

8.6. Todo descarte de informações confidencial, assim como, quaisquer dos recursos de tecnologia da informação e comunicação (recursos de TIC) que as contenham, devem passar por procedimentos de destruição que impossibilitem sua recuperação ou acesso por pessoas não autorizadas.

8.7. Todos os recursos de TIC da empresa devem ser utilizados com responsabilidade, com senha de bloqueio automático, antivírus, antispyware, firewall e mecanismos de controle de softwares maliciosos.

9. Diretrizes de Disponibilidade

9.1. Deve ser garantida a disponibilidade da informação.

9.2. Todo acesso a dados pessoais deve ser realizado com autorização expressa, por meio do uso de identidade digital (login e senha) pessoal e intransferível ou chaves de segurança fornecidas pela pessoa.

9.3. Toda informação deve ser armazenada em local apropriado e protegida contra acesso, modificação, destruição ou divulgação não autorizados.

9.4. Todas as identidades digitais dos usuários em todos os ativos e ambientes da empresa, em casos de desligamento, rescisão contratual ou término do contrato devem ser desativadas.

9.5. Deve ser estabelecido um plano para a realização e manutenção de cópias de segurança dos dados e informações, prevendo a redundância de servidores em locais diferentes.

10. Requisitos de Segurança da Informação

10.1. Deve ser estruturado e mantido um Sistema de Gestão de Segurança da Informação (SGSI) com o propósito de garantir o alinhamento dos objetivos, estratégias e planos de negócios da empresa, visando reduzir quaisquer possíveis incidentes que possam causar danos a confidencialidade, integridade e disponibilidade da informação.

10.2. O SGSI deve alinhar e organizar a segurança da informação e a continuidade de negócios, em conformidade com os requisitos legais, regulamentares e contratuais relevantes.

10.3. Deve ser garantido que o SGSI seja implementado de acordo com esta Política.

10.4. Deve ser estabelecido os papéis e responsabilidades de todos os usuários, funcionários, gestores e colaboradores da empresa.

10.5. Deve ser estabelecido e revisado periodicamente processos de controles e salvaguardas dos dados e informações, sendo determinado por uma Metodologia de Avaliação de Riscos e de Tratamento do Risco definidos pela empresa.

10.6. Deve ser confirmada a identidade do solicitante e a real necessidade do compartilhamento da informação solicitada, antes de ser repassada ou transmitida qualquer informação confidencial, seja de forma presencial, via telefone, comunicadores instantâneos, mensagens eletrônicas ou mídias sociais.

10.7. Deve ser elaborado um conjunto de estratégias e planos de ações de Continuidade do Negócio, para garantir que os serviços essenciais sejam preservados após a ocorrência de um desastre, danos ou possíveis falhas da infraestrutura tecnológica.

10.8. Para garantir a continuidade dos serviços, os recursos dos equipamentos devem ser constantemente monitorados, permitindo não só a identificação de possíveis problemas, mas também futuras atualizações de

acordo com a tendência de crescimento de seus programas e aplicativos.

10.9. Todo e qualquer documento, relatório, pesquisa, banco de dados, sistema e planilha deverá ser salvo em arquivo digital armazenado em Data Center fora da unidade da STT.

11. Disposições Finais

11.1. A PSI deve ser interpretada de forma restritiva, ou seja, casos excepcionais ou que não sejam por ela tratados só podem ser realizados após prévia e expressa autorização da Diretoria da STT.

11.2. Qualquer caso de exceção ou permissão diferenciada ocorrerá de forma pontual, aplicável apenas ao seu solicitante, dentro dos limites e motivos que a fundamentaram, cuja aprovação se dará por mera liberalidade da STT e com duração limitada, podendo ser revogada a qualquer tempo e sem necessidade de aviso prévio.

11.3. Quaisquer atitudes ou ações indevidas, ilícitas, não autorizadas ou contrárias ao recomendado por esta Política ou pelas demais normas e procedimentos de segurança da informação da STT serão consideradas violações por si só e estarão sujeitas às sanções previstas no Regimento Geral, contratos de prestação de serviços, contratos de trabalho e nas demais normas da empresa.

11.4. A PSI deve ser mantida atualizada no website da STT, bem como as demais normas de segurança da informação da empresa, em caso de indisponibilidade, podem ser solicitadas por meio do e-mail: administracao@sttorico.com.br.

11.5. Em caso de dúvidas quanto a esta Política ou aos demais procedimentos de segurança da informação da STT, quaisquer esclarecimentos devem ser solicitados pelo e-mail: administracao@sttorico.com.br.

11.6. Os casos de incidente, infração ou suspeita dessas ocorrências deverão ser comunicados imediatamente, pessoalmente ou pelo e-mail: administracao@sttorico.com.br.

11.7. Esta política passa a ter validade a partir de sua publicação no website da empresa.

11.8. Periodicidade de revisão da PSI será anual e concomitante à construção ou revisão dos Planos Estratégicos da Empresa ou extraordinariamente, a qualquer tempo.