**Política de Segurança**

1. Objetivo

1.1 Esta Política estabelece normas e diretrizes gerais de segurança da informação da SANTIS & FAGUNDES TECNOLOGIA LTDA (ou nome fantasia "INOVA TECH"), devendo ser observada por todos os seus colaboradores.

1.2 Esta política foi elaborada tendo por base o guia "Guia Orientativo Sobre Segurança da Informação Para Agentes de Tratamento de Pequeno Porte", elaborado pela Agência Nacional de Proteção de Dados (ANPD), destinado a startups e empresas de pequeno porte.

1.3 Esta Política é complementar à Política de Privacidade da SANTIS & FAGUNDES TECNOLOGIA, disponível nos diretórios institucionais da empresa, que trata da coleta e uso de dados.

2. Definições

2.1 Colaboradores: qualquer pessoa vinculada à empresa, independentemente do tipo do vínculo contratual mantido (empregado celetista, estatutário, prestador de serviços, autônomo, temporário, estagiário etc).

2.2 Informações: todo e qualquer dado, informação, projeto ou documento relativo à INOVA TECH, seus clientes, investidores, colaboradores ou que o colaborador tenha recebido ou venha a receber durante qualquer relação contratual com a INOVA TECH, independentemente de estarem classificados como confidenciais.

2.3 Segurança da Informação: Diretamente relacionada com proteção de um conjunto de dados, informações com objetivo de preservar o valor que possuem para indivíduo ou organização;

2.4 Incidente de Segurança da Informação: É um evento de segurança ou conjunto de eventos confirmados que impactem a disponibilidade, confidencialidade e integridade de um ativo de informação, assim como qualquer violação desta política;

2.5 Backup: É a cópia de segurança de dados de um dispositivo de armazenamento a outro para que possa ser restaurado em caso da perda dos dados originais;

2.6 Software: É a parte lógica, o conjunto de instruções e dados processados nos servidores e computadores;

2.7 Mídia removível: Dispositivos tais como Pendrive, Hd externo, CD capazes de armazenar informações;

2.8 Firewall: dispositivo de uma rede de computadores que tem por objetivo aplicar uma política de segurança a um determinado ponto da rede;

2.9 Stakeholder: grupos e indivíduos que, de uma forma ou de outra, apresentam algum nível de interesse nos projetos, atividades e resultados de uma determinada organização;

2.10 SaaS: Software como serviço, do inglês Software as a service, é uma forma de distribuição e comercialização de software.

3. Princípios

3.1 Confidencialidade: as informações, na INOVA TECH, independentemente da sua natureza, devem ser disponibilizadas somente a pessoas autorizadas e quando o acesso for estritamente necessário.

3.2 Integridade: sempre que possível, deve ser buscada a manutenção da exatidão e da completude das informações e os registros de versões e alterações dos documentos.

3.3 Disponibilidade: o acesso à informação pelos colaboradores que tenham acesso deve ser sempre contínuo e disponibilizado em plataformas e condições que assegurem padrões razoáveis de segurança da informação.

4. Diretrizes Gerais

4.1 Esta política é aplicável a todas as áreas e pessoas da INOVA TECH. Todos os colaboradores deverão, sempre antes de iniciar seu vínculo contratual com a INOVA TECH, assinar o Termo de Ciência desta Política, para confirmar que o conteúdo da Política foi compreendido e se refletirá em suas atitudes.

4.2 A INOVA TECH proverá aos colaboradores treinamentos e capacitações periódicas, oferecendo instruções e orientações sobre esta Política de Segurança da Informação.

4.3 Qualquer necessidade de esclarecimento ou dúvidas quanto a esta Política poderão ser levadas à diretoria da INOVA TECH ou ao time de Segurança da Informação, quando existente, que deverá prontamente elucidar e atuar sempre que necessário para garantir a conformidade desta Política.

4.4 É responsabilidade de todos os colaboradores a conduta correta e ética, obedecendo os preceitos de respeito às pessoas e preservação da imagem da INOVA TECH seu compromisso com a segurança da informação.

4.5 Espera-se ainda que os envolvidos cumpram com todos os requisitos da legislação brasileira aplicáveis, e comprometam-se a seguir integralmente os itens a seguir, mas não exclusivamente:

4.5.1 Proteger as informações contra acesso, modificação, destruição ou divulgação não autorizada, mantendo a sua confidencialidade, integridade e disponibilidade;

4.5.2 Exercer o trabalho profissional com responsabilidade, dedicação, honestidade e justiça, buscando sempre a melhor solução;

4.5.3 Esforçar-se para adquirir continuamente competências técnicas e profissionais, mantendo-se sempre atualizado com os avanços da profissão e especialidades;

4.5.4 Atuar dentro dos limites de sua competência profissional;

4.5.5 Guardar sigilo profissional por tempo indeterminado das informações que tiver acesso em razão do exercício de suas atividades contratadas;

4.5.6 Pautar sua relação com colegas nos princípios de consideração, respeito e solidariedade, assim como conduzir as atividades profissionais, que envolvam interação ou contribuição em grupo, sem discriminação de qualquer tipo, seja de cor, sexo, nacionalidade, idade, religião, estado civil ou qualquer outra condição humana;

4.5.7 Honrar compromissos e prazos estabelecidos;

4.5.8 Não praticar atos deliberados que possam comprometer segurança, privacidade ou que atentem para diminuição ou anulação de controles e proteções de segurança estabelecidos;

4.5.9 Comunicar imediatamente qualquer descumprimento desta Política de Segurança da Informação.

5. Regras Gerais

5.1 Os pontos a seguir representam as regras gerais de segurança da informação da INOVA TECH, e poderão ser complementadas por regras e regulamentos específicos aplicáveis a determinados procedimentos, se necessário.

5.2 As informações (em formato físico ou digital) e os ambientes tecnológicos utilizados pelos usuários são propriedade exclusiva da INOVA TECH, não podendo ser interpretados como de uso pessoal. Assim, os colaboradores da INOVA TECH desde já ficam cientes de que é expressamente proibida qualquer tipo de transferência dessas informações para ambientes não detidos e protegidos pela INOVA TECH. São exemplos desses ambientes:

5.2.1 Computadores, pendrives, HD's externos ou quaisquer dispositivos pessoais, de clientes ou fornecedores não fornecidos pela INOVA TECH;

5.2.2 Drivers virtuais vinculados a contas de e-mail pessoal ou não pertencentes à INOVA TECH;

5.2.3 Envios como anexos de e-mail a contas pessoais ou para finalidades que não sejam de interesse da INOVA TECH;

5.2.4 Upload de documentos em sites, formulários ou qualquer ambiente ou plataforma, exceto quando autorizadas expressamente por um representante da INOVA TECH ou quando o upload for procedimento de interesse da INOVA TECH.

5.3 As informações devem ser tratadas de forma ética e sigilosa e de acordo com as diretrizes estabelecidas pela governança corporativa da INOVA TECH e das leis vigentes.

5.4 Quaisquer informações de propriedade da INOVA TECH ou de terceiros mas sob gestão da INOVA TECH devem ser utilizadas somente para os fins autorizados e sempre no melhor interesse da empresa, seus clientes e fornecedores.

5.5 Todos os colaboradores da INOVA TECH, independentemente da relação contratual, devem ter ciência de que, o uso das informações e dos sistemas de informação, podem ser monitorados, sem aviso prévio, e que os registros assim obtidos podem servir de evidência para a aplicação de medidas de qualquer natureza, incluindo comerciais, estratégicas e disciplinares.

5.6 Os colaboradores da INOVA TECH devem possuir identificação única (física ou digital), pessoal e intransferível, que seja capaz de o qualificar como responsável por suas ações, em ambiente físico ou digital da INOVA TECH.

5.7 Os sistemas de informação da INOVA TECH realizam a autenticação de cada colaborador, autorizando seu acesso a funcionalidades conforme seu nível de acesso.

5.8 Somente profissionais autorizados, com vínculo contratual prévio e após a ciência do conteúdo desta política devem possuir acesso às informações.

5.9 Todo processo, sempre que possível, durante seu ciclo de vida, deve garantir a segregação de funções, identificando a participação de um ou mais colaboradores.

5.10 Os acessos devem sempre obedecer ao critério de menor privilégio, no qual os usuários devem possuir somente as permissões necessárias para a execução de suas atividades.

5.11 Os sistemas de informação da INOVA TECH realizam o registro das operações efetuadas de forma a permitir auditorias futuras de operações realizadas por cada colaborador.

5.12 Os colaboradores são responsáveis pela salvaguarda e confidencialidade de informações e senhas que possuam durante o exercício do seu cargo. Além de eventuais regulamentos e políticas específicas, são boas práticas de segurança de senhas e da informação:

5.12.1 Manter softwares e sistemas operacionais sempre atualizados;

5.12.2 Adotar ferramentas de gestão de proteção contra incidentes cibernéticos (antivírus, por exemplo), além de backups e cópias de segurança;

5.12.3 Investir em soluções de segurança que apontem vulnerabilidades na infraestrutura e nos sistemas internos da empresa;

5.12.4 Implementar políticas específicas de segurança da informação, com disposições adequadas à prática da empresa e com documentação de protocolos e procedimentos;

5.12.5 Adotar mecanismos de bloqueio de saída de arquivos e informações (ex.: bloqueios a e-mails pessoais e ao reconhecimento de pendrives pelos computadores da empresa);

5.12.6 Definir métricas e dados de avaliação da segurança da informação da empresa.

5.12.7 Sempre que possível utilizar autenticação de dois fatores e senhas com alta complexidade para acesso aos sistemas.

5.13 As responsabilidades no que tange à garantia dos princípios devem ser amplamente divulgadas, fazendo valer firmemente a aplicação das normas aqui descritas.

5.14 As informações devem ser utilizadas de forma transparente e apenas para a finalidade para a qual foram coletadas e/ou para usos estatísticos sem expor os clientes de forma identificável.

5.15 Não discutir nem mencionar informações confidenciais fora do ambiente de trabalho, assim entendido o ambiente físico da empresa e os canais oficiais de comunicação corporativa, protegidos pelas regras e procedimentos mencionados nesta política. São exemplos de ambientes inadequados para discussões ou qualquer tipo de menção a informações confidenciais:

5.15.1 Meios de transporte (ônibus, Uber, aviões etc.);

5.15.2 Festas e confraternizações da empresa;

5.15.3 Happy Hours;

5.15.4 Bares e restaurantes;

5.15.5 Casas de familiares, amigos e conhecidos.

5.16 Para assegurar maior clareza e segurança, a gestão da INOVA TECH poderá adotar um modelo de rotulagem da informação de acordo com o grau de confidencialidade e caráter estratégico de um documento ou informação, na forma seguinte:

| | **Definição** | **Tratamento** |
|---|---|---|
| Estratégica | Informação relativa a planos estratégicos, operacionais, financeiros ou de produtos, segredos de negócio, transações de fusões e aquisições de empresas, relatórios ou documentos que contenham resultados financeiros, técnicos ou operacionais, bases de dados, tratadas ou não, de clientes, usuários, parceiros, concorrentes ou empregados, ou qualquer informação que, se publicada fora dos ambientes internos de comunicação da INOVA TECH, poderão ocasionar prejuízos significativos à INOVA TECH. | Acesso restrito a diretores, conselheiros e pessoas-chave dos times da área relacionada à informação. Só poderão ser classificadas como Públicas após aprovação da Diretoria da INOVA TECH; |
| Interna | Qualquer informação não classificada como Estratégica ou Pública. | Regras comuns de segurança da informação |
| Pública | Informação declarada por escrito como pública por membro dos times de Marketing, Relações Públicas, da Diretoria ou do Conselho de Administração da INOVA TECH. Somente as informações desta categoria poderão ser divulgadas fora dos canais oficiais de comunicação da INOVA TECH. | Poderão ser divulgadas conforme definido pelos times de Marketing ou de Relações Públicas. |

5.17 A classificação das informações de acordo com a tabela acima deverá ser feita de forma discricionária pelo gestor da área responsável pela criação ou manuseio da informação.

6. Segurança no Desenvolvimento de Sistemas

6.1 Todo o processo de desenvolvimento de software na INOVA TECH é orientado a evitar, encontrar e corrigir vulnerabilidades que possam comprometer os Princípios de Segurança da Informação.

6.2 O software e suas versões serão armazenados em repositórios com níveis de controle de acesso e gestão de modificações.

6.3 Revisões de código são realizadas para validar a integridade e prevenir erros, seja involuntário ou intencional, utilizando de dados fictícios ou anonimização e em ambiente não produtivo.

7. Gestão de Vulnerabilidade

7.1 Prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético, deve ser um trabalho de toda a equipe de desenvolvimento da IN 19, sendo realizadas medidas como a aplicação de patches de segurança, atualizações de sistemas operacionais e softwares nos dispositivos dos colaboradores envolvidos.

7.2 A diretoria técnica da INOVA TECH (CTO) e/ou o encarregado de Segurança da Informação deve promover a realização periódica de avaliações de segurança como testes de penetração e avaliações de vulnerabilidade com periodicidade semestral.

8. Backup e restauração

8.1 Não é permitida a cópia de dados confidenciais para processamento ou armazenamento em serviços externos, de terceiros não autorizados pela INOVA TECH.

8.2 A INOVA TECH utiliza-se de infraestrutura de nuvem que garante o backup do banco de dados, com rotinas diárias de validação sendo realizadas por nosso time interno, além disso, anualmente realizamos testes para garantir a nossa capacidade de restauração das informações de nossos clientes

8.3 Todos os arquivos devem ser gravados em nuvem para garantia de acesso e backup.

8.4 Alguns backups têm tempo de vida determinado por lei, portanto a equipe responsável pelos backups deve ser informada e zelar por mantê-los disponíveis durante esse tempo, bem como os equipamentos necessários para sua recuperação quando necessário.

9. Notificação de Incidentes de Segurança da Informação

9,1 Qualquer descumprimento ou violação desta política, bem como incidentes de qualquer natureza relacionados à segurança da informação, deverá ser comunicado imediatamente ao responsável da INOVA TECH, através do email adm@inovachat.com.br, ou à diretoria técnica da empresa (CTO).

9.2 Os procedimentos a serem aplicados aos casos de descumprimento desta Política ou a publicações de informações em desacordo com as diretrizes de classificação serão definidos pelo time de compliance da INOVA TECH ou pela diretoria da empresa.

10. Gestão desta Política

10.1 A diretoria técnica da INOVA TECH (CTO) e/ou o encarregado de Segurança da Informação, quando existente, serão responsáveis pela observância desta política nas operações das empresas, sendo seu dever a remessa de casos de descumprimento à diretoria da INOVA TECH.

10.2 Esta política tem validade por tempo indefinido, devendo ser revista anualmente.

DATA DA PUBLICAÇÃO: 02/07/2024