Política de Segurança da Informação para Fornecedores

tecnoAtiva Consultoria e Sistemas LTDA.

Sumário

1. Objetivos

O principal objetivo desta política é orientar os fornecedores da tecnoAtiva sobre as diretrizes de segurança da informação aplicáveis, descrevendo sua participação e responsabilidade enquanto fornecedor. Visando assegurar que os usuários tenham acesso à informação com a qualidade necessária para o desempenho de suas atividades, ao mesmo tempo em que se previne a perda de dados e o acesso não autorizado às informações.

2. Escopo

Aplica-se a todos os fornecedores e parceiros da organização.

3. Vigência

Essa política passa a vigorar a partir da data da publicação.

4. Diretrizes Gerais

4.1. Princípios de Segurança da Informação

Todos os fornecedores da Organização devem demonstrar compromisso com a política de segurança da informação, garantindo a proteção e o uso adequado dos recursos informacionais. Além disso, devem empenhar-se na manutenção e proteção dos princípios fundamentais de segurança da informação:

- **Confidencialidade** – O Fornecedor é responsável por assegurar o sigilo e a restrição de acesso às informações compartilhadas ou acessadas no desempenho de suas funções e serviços contratados. Todas as informações disponibilizadas ou acessíveis ao Fornecedor devem ser tratadas como confidenciais e consideradas propriedade exclusiva da Organização.

- **Integridade** – Fornecedor deve utilizar os ativos da Organização, incluindo informações, de forma adequada e conforme as autorizações concedidas. É estritamente proibida qualquer manipulação ou alteração de ativos de informação fora do escopo de trabalho definido ou das limitações estabelecidas por procedimentos e controles de acesso nos sistemas de informação.

- **Disponibilidade** – O Fornecedor compromete-se a preservar os ambientes e recursos tecnológicos da Organização sob sua responsabilidade ou suporte, garantindo a continuidade e a prestação ininterrupta dos serviços.

4.2. Conduta

Espera-se dos Fornecedores um comportamento ético e de elevado moral, respeito e a observância às leis vigentes assim como dos regulamentos da Organização, incluindo:

- Exercer o trabalho profissional com responsabilidade, dedicação, honestidade e justiça, buscando sempre a melhor solução;
- Atuar dentro dos limites de sua competência profissional;
- Guardar sigilo profissional das informações que tiver acesso em razão do exercício de suas atividades contratadas;
- Atender às expectativas de confiança depositadas pela Organização, acessando e utilizando recursos e informações apenas no limite da necessidade para realização de seu trabalho e autorização concedida;
- Não praticar atos deliberados que possam comprometer segurança, privacidade ou que atentem para diminuição ou anulação de controles e proteções de segurança estabelecidos pela Organização.

4.3. Continuidade de Negócio

O fornecedor deve assegurar a existência de processos para continuidade de negócios e gestão de incidentes de segurança para proteção, detecção, resposta e recuperação contra-ataques cibernéticos.

Quando acionados em cenário de contingência, ativação de planos de continuidade e/ou recuperação de desastres, os Fornecedores responsáveis por ações de emergência devem priorizar as ações conforme nível de prioridade classificado pela Organização, respeitando os Acordos de Nível de Serviço (ANS) definidos em contrato.

5. Orientações Específicas

De forma geral, a tecnoAtiva baseia sua estratégia de Segurança da Informação na norma ISO 27001. É de responsabilidade do Fornecedor a observância destas normativas, ainda que não explicitamente contidas nesta política específica. Para isso, o Fornecedor deve buscar, sempre que não encontrar orientação suficiente neste documento, instruções específicas junto à Organização e complementar o entendimento dos requisitos de segurança da informação, se necessário.

A seguir, estão detalhadas as diretrizes específicas de segurança da informação que os fornecedores devem observar, sempre que aplicável.

5.1. Controle de Acesso

- Sistemas de informação fornecidos por Fornecedores da Organização, para uso de colaboradores da Organização devem oferecer autenticação segura e prover meios de rastreabilidade de ações realizadas.

- Os Fornecedores devem utilizar ativos de informação apenas para o propósito relacionado a sua atuação contratada.

- Em caso de atuação presencial, os Fornecedores devem atuar e transitar apenas em locais expressamente autorizados e relacionados a sua atuação contratada.

- Cabe ao fornecedor ter procedimentos de controle de acesso aos dados que forem fornecidos pela organização, a fim de prevenir o acesso não autorizado e o vazamento de dados.

5.2. Tratamento de Mídia

- O fornecedor de serviços deverá estabelecer um procedimento seguro para o tratamento das mídias (discos rígidos internos/externos, drives de memória etc.), considerando o descarte de forma a fim de prevenir a divulgação não autorizada de dados.

5.3. Segurança de Serviços de Rede

- Cada serviço de rede, seja local ou terceirizado, deve incluir mecanismos de segurança (proteção, detecção e reação) adaptados à sensibilidade dos dados sendo transmitidos. Esses mecanismos de

segurança devem ser implementados na rede ou diretamente nos sistemas, aplicativos, estações de trabalho e/ou banco de dados.

- Todas as transferências de dados devem ser realizadas por ferramentas explicitamente validadas por equipe tecnicamente qualificada à escolha e responsabilidade do fornecedor.

5.4. Backup de Informações e Sistemas

As políticas de *backup* e *restore* devem ser definidas para os dados, *software* e sistemas que tratam dados.

5.5. Relações com Terceiros

Os serviços entregues por terceiros devem seguir as diretrizes estabelecidas nesta política, sendo de total responsabilidade do fornecedor de serviços a garantia pelo cumprimento dos serviços e de todas as obrigações contratuais e legais.

5.6. Gestão de Incidentes

Os incidentes de Segurança da Informação devem ser identificados e gerenciados por processos consistentes, disciplinados e compartilhados.

No caso de um incidente de Segurança da Informação, a equipe responsável do fornecedor deve realizar a pronta comunicação e a coordenação do esforço coletivo até que o incidente seja declarado encerrado.

Assim que identificados, o mais rápido possível, todos os incidentes de segurança devem ser notificados e comunicados a equipe de TI da tecnoAtiva, através do e-mail **servicedesk@tecnoativa.com.br**.

5.7. Observância de Leis e Normas

As atividades do fornecedor de serviços devem garantir a observância das obrigações contratuais, estatutárias e regulatórias para assegurar que as devidas exigências de segurança sejam levadas em conta em seus processos, limitado a sua atuação contratada.

Aos fornecedores que tratam dados pessoais, a tecnoAtiva deve garantir que os dados pessoais sejam gerenciados de acordo com a Lei 13709 de 14 de agosto de 2019 – Lei Geral de Proteção de Dados Pessoais, quando nenhuma outra orientação for passada.

5.8. Violações

Qualquer evento que resultar em roubo, perda, uso não autorizado, divulgação não autorizada, destruição não autorizada, ou ainda, serviços degradados ou recusados de ativos da informação, implica uma violação da Segurança da Informação.

No caso de violação desta política ou das demais políticas relacionadas à segurança da informação, a tecnoAtiva poderá advertir o fornecedor, podendo até rescindir o contrato.

5.9. Revisão e atualização

Este documento será revisado anualmente, e a qualificação dos fornecedores será reavaliada a cada 2 anos.

HISTÓRICO DE ALTERAÇÃO

VERSÃO	DATA	NOME	AÇÃO (Elaboração, Revisão, Atualização, Aprovação)	CONTEÚDO
1.0	17/06/2025	Wesley Ramos	Elaboração	Primeira versão
		Andrea Campelo	Aprovação	