Medidas Técnicas e Organizacionais SONDA

A SONDA implementará as medidas descritas abaixo, desde que as medidas contribuam direta ou indiretamente ou possam contribuir para a proteção de Dados Pessoais no âmbito do Contrato Original celebrado entre as partes para o tratamento de dados.

As medidas técnicas e organizacionais implementadas pela SONDA são baseadas nas melhores práticas de mercado através dos modelos da ISO27K e ISAE3402. As Medidas Técnicas e Organizacionais estão sujeitas ao progresso e desenvolvimento técnico. A este respeito, a SONDA está autorizada a implementar medidas alternativas adequadas. O nível de segurança deverá estar alinhado com as melhores práticas de segurança do setor e não menos do que as medidas aqui estabelecidas. Todas as principais alterações deverão ser acordadas com o CONTRATANTE e documentadas.

As Medidas Técnicas e Organizacionais incluídas neste documento são medidas aplicáveis ao(s) Serviço(s) prestado(s) pela SONDA. Se necessário para o Serviço a SONDA pode incluir outras medidas técnicas e organizacionais na Ordem de Serviço ou Especificação de Serviço.

1. Gestão de riscos e procedimentos para validação, revisão e avaliação

i. A SONDA identifica e avalia os riscos de segurança relacionados à confidencialidade, integridade e disponibilidade. Com base nessa avaliação, implementa medidas técnicas e organizacionais adequadas para garantir um nível de segurança adequado ao risco.

ii. A SONDA adota processos e rotinas documentadas para lidar com os riscos em suas operações ao tratar dados pessoais em nome do CLIENTE.

iii. A SONDA avalia periodicamente os riscos relacionados aos sistemas de informação e tratamento, armazenamento e transmissão de informações.

iv. A SONDA identifica e avalia os riscos de segurança relacionados à confidencialidade, integridade e disponibilidade e, com base em tal avaliação, implementa medidas técnicas e organizacionais adequadas para garantir um nível de segurança adequado ao risco dos tipos e finalidades de Dados Pessoais específicos sendo tratados pela SONDA, incluindo, entre outros, conforme o caso:

   a. a capacidade de garantir a confidencialidade, integridade, disponibilidade e resiliência contínuas dos sistemas e serviços de tratamento;

   b. a capacidade de restaurar a disponibilidade e o acesso aos dados do CLIENTE em tempo hábil no caso de um incidente físico ou técnico;

   c. um processo para testar regularmente, avaliar e avaliar a eficácia das medidas técnicas e organizacionais para garantir a segurança do tratamento.

v. A SONDA avalia periodicamente os riscos relacionados aos sistemas de informação e tratamento de dados pessoais (por exemplo, ao armazenar e transmitir dados pessoais).

vi. A SONDA monitora, revisa e audita regularmente a conformidade do Suboperador com as Medidas Técnicas e Organizacionais. Ainda, a pedido do CLIENTE, a SONDA fornece ao CLIENTE evidências sobre a conformidade do Suboperador com as Medidas Técnicas e Organizacionais.

vii. A SONDA funciona de acordo com os princípios de proteção de dados desde o projeto e por padrão e deverá fornecer documentação suficiente da implementação da proteção de dados desde o projeto e por padrão.

2. Medidas Organizacionais

A organização interna do operador de dados deverá atender aos requisitos específicos de proteção de dados.

A. Políticas e Gerenciamento de Políticas

i. A SONDA adota um sistema de gestão de segurança da informação (SGSI) definido e documentado, incluindo uma política e procedimentos de segurança da informação em vigor, aprovados pela administração da SONDA. Estes estão publicados dentro da organização da SONDA e foram comunicados aos colaboradores envolvidos na prestação dos serviços.

ii. A SONDA revisa periodicamente as políticas e procedimentos da SONDA relativos à proteção de dados e segurança da informação e atualiza-os, se necessário, para garantir a sua conformidade com as Medidas Técnicas e Organizacionais e o ADITIVO.

B. Organização de Proteção de Dados e Segurança da Informação

i. A SONDA indica pelo menos um encarregado pelo tratamento de dados pessoais com as competências adequadas e que atua como o principal contato para a proteção de dados.

ii. A SONDA possui funções e responsabilidades de segurança definidas e documentadas em sua organização.

C. Requisitos Organizacionais

i. A SONDA garante que os seus colaboradores e prestadores de serviço trate as informações de acordo com o nível de confidencialidade exigido pelo ADITIVO e que tenha o compromisso por escrito dos funcionários de manter a confidencialidade.

ii. A SONDA garante que os colaboradores envolvidos na prestação de serviço estejam cientes do uso aprovado (incluindo restrições de uso,

conforme o caso) de informações, instalações e sistemas nos termos do ADITIVO.

iii. A SONDA garante que os seus colaboradores envolvidos na prestação dos serviços nos termos do ADITIVO sejam confiáveis, atendam aos critérios de segurança estabelecidos e tenham sido, durante o prazo da atribuição, sujeitos a uma triagem adequada e verificação de antecedentes (se permitido pela lei aplicável).

iv. A SONDA garante que os colaboradores envolvidos nas responsabilidades de segurança estejam adequadamente treinados para realizar as tarefas relacionadas à segurança.

v. A SONDA fornece e garante treinamento periódico de conscientização para os colaboradores envolvidos na prestação de serviço.

3. Confidencialidade

A. Controle de Acesso (Segurança física)

i. A SONDA protege as instalações de tratamento de informações que abrange especificamente as atividades de controle, vigilância e manutenção de infraestrutura e instalações (espaço físico, controle perimetral, ameaças ambientais e continuidade do serviço de eletricidade) necessários para a prestação adequada de serviços aos nossos clientes.

ii. A SONDA protege os bens contra roubo, manipulação e destruição.

iii. A SONDA especifica os indivíduos autorizados permitidos em suas instalações de tratamento e possui um processo de controle de acesso.

iv. Medidas adicionais para Data Centers:

a. O Sistema de Gestão da Segurança da Informação suporta a provisão dos serviços de Infraestrutura & Operação de Datacenter e Cloud Computing, abrange especificamente as atividades de controle, vigilância e manutenção de infraestrutura e facilities (espaço físico, controle de perímetro, ameaças ambientais e continuidade de serviços elétricos) necessários para provisão adequada de serviços para os nossos clientes.

b. Apenas representantes autorizados têm acesso aos sistemas e infraestrutura dentro das instalações do Data Center.

c. Para proteger a funcionalidade adequada, os equipamentos de segurança física (por exemplo, sensores de movimento, câmeras etc.) passam por manutenção regularmente.

d. A SONDA e todos os provedores de Data Centers terceirizados registram os nomes e horários dos colaboradores e prestadores de serviço autorizados que entram nas áreas privadas da SONDA dentro dos Data Centers.

B. Controle de acesso (Lógico)

i. A SONDA adota uma política de controle de acesso definida e documentada para instalações, sites, rede, sistema, aplicativo e acesso a informações/dados (incluindo controles de acesso físico, lógico e remoto), um processo de autorização para acesso de usuário e privilégios, procedimentos para revogar acesso direitos e um uso aceitável de privilégios de acesso para os colaboradores e prestadores de serviço da SONDA no local.

ii. A SONDA adota um registro de usuário formal e documentado e um processo de cancelamento de registro implementado para permitir a atribuição de direitos de acesso.

iii. A SONDA atribui todos os privilégios de acesso com base no princípio da necessidade de tomar conhecimento e no princípio do menor privilégio.

iv. A SONDA utiliza autenticação forte (multifatorial) para usuários de acesso remoto e usuários que se conectam a partir de uma rede não confiável.

v. A SONDA garante que seus colaboradores e prestadores de serviço tenham um identificador pessoal e único (ID do usuário) e adotem uma técnica de autenticação adequada, que confirma e garante a identidade dos usuários.

D. Diretrizes sobre a admissão nas instalações do CLIENTE e/ou instalações SONDA

A autorização de acesso às instalações e propriedades (como edifícios de datacenter, edifícios de escritórios, locais técnicos) está sujeita ao seguinte:

i. A SONDA segue os regulamentos locais (como regulamentos para "áreas restritas") para as instalações do CLIENTE ao realizar as cessões nos termos do Contrato Original.

ii. Os colaboradores da SONDA portam crachá funcional ou, no caso de visitantes, um crachá de visitante, visível o tempo todo durante o trabalho.

4. Segurança das operações

i. A SONDA dispõe de um sistema de gerenciamento de mudanças estabelecido para fazer mudanças nos processos de negócios, instalações e sistemas de tratamento de informações.

ii. A rede da SONDA é protegida da rede pública por firewalls.

iii. A SONDA realiza cópias de backup de informações críticas e testar cópias de backup para garantir que as informações possam ser restauradas conforme acordado com o CLIENTE.

iv. A SONDA registra e monitora as atividades, como criar, ler, copiar, alterar e excluir os dados tratados, bem como exceções, falhas e eventos de segurança da informação e revisa-os regularmente. Além disso, a SONDA protege e armazena (por pelo menos 6 meses ou durante o(s) período(s) definido(s) pela Legislação de Proteção de Dados) informações de registro e, mediante solicitação, fornece dados de monitoramento ao CLIENTE. Anomalias/incidentes/indicadores de comprometimento são reportados de acordo com os requisitos de gestão de violação de dados conforme estabelecido abaixo.

v. A SONDA gerencia vulnerabilidades de todas as tecnologias relevantes, como sistemas operacionais, bancos de dados, aplicativos de forma proativa e em tempo hábil.

vi. A SONDA estabelece linhas de base de segurança (reforço) para todas as tecnologias relevantes, como sistemas operacionais, bancos de dados, aplicativos.

5. Integridade

i. A SONDA implementa controles de segurança de rede, como nível de serviço, firewall e segregação para proteger os sistemas de informação.

ii. A SONDA opera um sistema de detecção de phishing e SPAM com o objetivo de proteger seus CLIENTEs e a SONDA (e os Dados Pessoais dos quais as partes são o Controlador) contra conteúdo indesejado e a propagação de SPAM/phishing e cumprir os requisitos do operador e a legislação aplicável.

iii. Os Dados Pessoais tratados em nome são tratados exclusivamente de acordo com o Contrato Original e as instruções do controlador para o operador.

iv. A SONDA trabalha de acordo com instruções escritas ou acordos e documentos pertencentes a esse ADITIVO.

6. Gerenciamento de violação de dados

i. A SONDA estabelece procedimentos para gerenciamento de violação de dados.

ii. A SONDA informa ao CLIENTE sobre qualquer violação de dados (incluindo, mas não se limitando a incidentes relacionados ao tratamento de dados pessoais) o mais rápido possível.

7. Gestão de Continuidade dos Negócios

i. A SONDA identifica os riscos de continuidade dos negócios e tomar as medidas necessárias para controlar e mitigar esses riscos.

ii. A SONDA dispõe de processos e de rotinas documentados para lidar com a continuidade dos negócios.

iii. A SONDA garante que a segurança da informação seja incorporada aos planos de continuidade de negócios.