HITACHI
Inspire the Next

ANEXO D
REQUISITOS DE SEGURANÇA DA INFORMAÇÃO

1. Introdução

Estes Requisitos de Segurança da Informação (o "ISR") refletem o acordo das Partes com relação aos padrões mínimos que o Fornecedor deverá empregar durante todo o período do Contrato de Serviços Profissionais, incluindo quaisquer SOWs (coletivamente, o "**MPSA**").

2. Definições

A menos que expressamente definido neste ISR, todos os termos em maiúsculas terão o mesmo significado que no MPSA. Neste ISR, os seguintes termos têm os seguintes significados:

Ambiente de Produção: Sistemas do Fornecedor, usado para fornecer Serviços ou Entregáveis à Hitachi.

Ambiente de Teste e Desenvolvimento: Sistemas do Fornecedor usados com a finalidade de desenvolvimento e/ou teste de um serviço, mas não usados diretamente para entregar Serviços ou Entregáveis à Hitachi ou ao Cliente da Hitachi.

Dados da Hitachi: quaisquer Dados da Hitachi, incluindo, mas não se limitando a, dados compartilhados ou pertencentes ao MPSA, Serviços, Entregáveis, faturamento e processos de negócios. Os Dados da Hitachi inclui dados dos Clientes da Hitachi.

Dados Restritos da Hitachi: Dados Hitachi classificados como restritos, e que exijam um nível de proteção elevado, incluindo, mas não se limitando a, informações pessoais, propriedade intelectual, planos financeiros e outras informações confidenciais.

Sistemas Hitachi: quaisquer redes, sistemas de computação, aplicativos, serviços em nuvem da Hitachi, que forneçam acesso ou armazenem, processem ou transmitam Dados da Hitachi.

Sistemas do Fornecedor: Redes de fornecedores, sistemas de computação, aplicativos e/ou serviços em nuvem que acessam, fornecem acesso, armazenam, processam ou transmitem Dados da Hitachi ou acessam Sistemas Hitachi.

3. Requerimentos Gerais

(a) O Fornecedor manterá salvaguardas organizacionais, físicas e técnicas que atendam ou excedam as melhores práticas da indústria - por exemplo, conforme estabelecido na ISO/IEC 27001: 2013/27002: 2013 ou NIST SP 800-53 e fornecerá à Hitachi uma cópia da documentação de seu programa de segurança da informação e práticas mediante solicitação.

(b) O Fornecedor manterá um programa de segurança da informação sob a supervisão de um Diretor de Segurança da Informação (CISO) ou um líder sênior que seja responsável por um programa de segurança da informação eficaz e exerça a supervisão necessária e apropriada sobre o Pessoal, para manter a confidencialidade, integridade, disponibilidade adequada, e segurança dos sistemas do Fornecedor.

(c) O Fornecedor entregará, durante o prazo do MPSA, um relatório SOC 2 Tipo II ou certificação ISO/IEC 27001:2013 com Declaração de Aplicabilidade associada ou um atestado ou certificação equivalente, de um terceiro independente cobrindo sua operação referente aos Serviços ou Entregáveis.

4. Gerenciamento de Terceiros

(a) O Fornecedor deverá avaliar os riscos de segurança da informação associados a serviços de terceiros que sejam necessários para a entrega dos Serviços ou Entregáveis e identificará ações corretivas para mitigar tais riscos. Os serviços existentes de terceiros devem ser monitorados e avaliados periodicamente quanto aos riscos de segurança da informação e medidas de mitigação de riscos devem ser tomadas pelo Fornecedor.

(b) O Fornecedor deverá divulgar com antecedência os nomes de quaisquer subcontratados terceirizados que possam acessar, processar, armazenar ou transmitir Dados da Hitachi.

5. Segurança de Pessoal

(a) O Fornecedor deverá garantir que todo o Pessoal com acesso a aos Dados ou Sistemas da Hitachi seja submetido a um treinamento formal de conscientização sobre segurança da informação, anualmente.

(b) O Fornecedor garantirá que todo o Pessoal com acesso a Dados ou Sistemas da Hitachi tenha passado por uma verificação de antecedentes adequada antes de acessar os Dados e Sistemas da Hitachi.

6. Controle de Acesso

(a) O Fornecedor deverá proteger o acesso aos Dados e Sistemas da Hitachi e aos Sistemas Fornecedor relevantes por técnicas que estejam em conformidade com os padrões e diretrizes da indústria de segurança, como, por exemplo, senhas fortes ou autenticação multifator (MFA).

(b) O acesso aos Dados da Hitachi é concedido estritamente com base nas necessidades comerciais.

(c) O Fornecedor deverá garantir que todo o Pessoal que está se conectando remotamente (de fora das instalações do Fornecedor) para acessar Dados e Sistemas da Hitachi ou Sistemas Fornecedor sejam autenticados usando autenticação multifator e conexões remotas criptografadas.

7. Sistemas de Segurança

O Fornecedor deverá usar meios técnicos e procedimentais para proteger continuamente os Sistemas do Fornecedor, incluindo, mas não se limitando a:

(a) anti-malware, proteção avançada contra ameaças;

(b) *firewalls*, *gateways* seguros, segurança de acesso à rede, sistemas de prevenção de intrusão (IPS), sistemas de detecção de intrusão (IDS);

(c) proteção e configuração segura dos Sistemas do Fornecedor;
(d) varreduras periódicas de vulnerabilidades e remediação de vulnerabilidades proporcionais à gravidade das vulnerabilidades;
(e) *patching* de *firmware*, sistema operacional, *middleware*, aplicativos para o *patch* mais recente disponível;
(f) teste de penetração de Sistemas do Fornecedor acessíveis externamente pelo menos uma vez por ano; e
(g) registrar, monitorar e responder a eventos de segurança da informação e condições anormais.

8. Proteção de Dados

O Fornecedor deverá garantir que os seguintes controles técnicos e procedimentais estejam em vigor para proteger os Dados da Hitachi, a menos que previamente aprovado pela Hitachi por escrito:
(a) Os Dados da Hitachi serão armazenados e processados física ou logicamente separados dos de outros clientes do Fornecedor e separados de outros Ambientes do Fornecedor.
(b) Os dados Restritos da Hitachi serão sempre criptografados quando armazenados em repouso, inclusive na mídia de armazenamento de backup ou quando armazenados de forma efêmera durante o trânsito, usando métodos de criptografia fortes.
(c) Os Dados Hitachi serão criptografados quando em trânsito (transmitidos) usando métodos e protocolos de criptografia fortes e seguros usados (especificamente TLS 1.2 e superior).
(d) O acesso aos Dados e Sistemas Hitachi será concedido estritamente com base na necessidade de conhecê-los e o acesso será imediatamente revogado quando não for mais necessário.
(e) O acesso programático aos Dados e Sistemas da Hitachi será protegido por tokens ou certificados de autenticação, os quais serão alternados regularmente.
(f) Os Ambientes de Produção são separados dos Ambientes de Teste e Desenvolvimento e os dados da Hitachi serão separados. As atividades de teste e desenvolvimento não serão realizadas em Ambientes de Produção e os Dados da Hitachi não serão armazenados em nenhum Ambiente de Produção.
(g) Todos os Dados da Hitachi, que sejam utilizados para teste ou desenvolvimento, serão protegidos de forma adequada, ou seja, usando apenas dados de teste (não dados de produção) ou mascarando ou ofuscando os dados de produção.
(h) O acesso aos Dados da Hitachi será registrado e os logs serão mantidos por pelo menos 1 (um) ano.
(i) Nenhum Dado Restrito da Hitachi será armazenado em mídia pessoal removível, como discos rígidos portáteis, unidades USB, DVDs, etc.
(j) Nenhum Dado Restrito da Hitachi será armazenado em serviços de nuvem de terceiros sem aprovação prévia por escrito da Hitachi.
(k) Se o Fornecedor armazenar Dados da Hitachi, eles e os Sistemas do Fornecedor possuirão *backup* para oferecer suporte de Ponto de Recuperação (RPO) e Objetivo de Tempo de Recuperação (RTO) dos Produtos e Serviços, conforme: (1) especificado no MPSA; ou (2) com RPO de 24 horas e RTO de 24 horas, o que for menor.
(l) Todos os Dados da Hitachi, incluindo mídia contendo Dados da Hitachi, deverão ser devolvidos à Hitachi ou totalmente após o encerramento do MPSA ou de uma SOW aplicável.

9. Segurança do Aplicativo

O Fornecedor deverá garantir que as práticas de segurança do sistema e do aplicativo estejam em vigor para todos os softwares e serviços online fornecidos à Hitachi, incluindo, mas não se limitando às seguintes práticas:
(a) Garantir que os desenvolvedores sejam qualificados e treinados em aplicações seguras e técnicas de desenvolvimento de sistemas.
(b) Aplicar práticas de codificação seguras (por exemplo, OWASP Top 10 ou CMM SEI CERT Coding Standards).
(c) Aplicar modelagem de ameaças a aplicativos e sistemas.
(d) Aplicar análise estática do código-fonte.
(e) Realizar testes de penetração.
(f) Realizar análise de composição de software de terceiros.
(g) Executar Verificações de Segurança de aplicativos da Web Dinâmicos Autenticados.
(h) Informar prontamente a Hitachi sobre quaisquer vulnerabilidades de segurança, juntamente com sua classificação CVSS, que tenham sido encontradas por escrito ou em uma publicação acessível à Hitachi.
(i) Corrigir as vulnerabilidades de segurança encontradas durante o teste em 15 dias (Crítico), 30 dias (Alto), 60 dias (Moderado) e 90 dias (todos os outros níveis de gravidade).
A qualquer momento e a pedido exclusivo da Hitachi, o Fornecedor deverá fornecer à Hitachi a documentação de suas práticas de segurança de aplicativos.

10. Segurança Física

(a) O Fornecedor deverá garantir que os Dados da Hitachi sejam armazenados, processados e acessados apenas por Pessoal autorizado, em um ambiente seguro.
(b) O Fornecedor deverá garantir que todas as mídias contendo Dados da Hitachi sejam armazenadas e acessadas por Pessoal autorizado, em um ambiente seguro.

(c) O Fornecedor deverá garantir que os Sistemas do Fornecedor só possam ser removidos ou adicionados com autorização da gestão do Fornecedor.
(d) O Fornecedor deverá garantir que sua força de trabalho remota seja treinada e obrigada a aplicar práticas seguras ao trabalhar remotamente.

11. Relatar Incidentes de Segurança

(a) O Fornecedor deverá relatar incidentes de segurança que afetem a Hitachi Data ou os Sistemas da Systems dentro de 24 horas, no mínimo, e nenhum caso poderá exceder 48 horas, por e-mail para cybersecurity@hitachivantara.com.
(b) O Fornecedor deverá fornecer um e-mail ou ponto de contato telefônico para consultas de segurança e acompanhamento de incidentes pela Hitachi antes do início dos Serviços.