HUGHES
An EchoStar Company

Diretrizes Para Fornecedores

Disposições Relativas à Segurança da Informação

1. Com o objetivo de garantir o cumprimento de suas obrigações legais, regulatórias e contratuais relacionadas à confidencialidade, integridade e disponibilidade das informações direta ou indiretamente relacionadas à sua atuação no âmbito deste Contrato, sempre que aplicável e condizente com o objeto do contrato, a CONTRATADA compromete-se a envidar seus melhores esforços para implementar medidas técnicas e administrativas relacionadas à segurança da informação, conforme disposições abaixo;

2. Manutenção e implementação de políticas de segurança da informação que promovam aspectos de confidencialidade, integridade e disponibilidade da informação, de forma compatível com a legislação aplicável ou em linha com a norma ISO/IEC 27001 e/ou padrões equivalentes;

3. Realização de treinamentos periódicos e demais iniciativas de conscientização e capacitação sobre proteção segurança da informação com seus colaboradores e terceiros contratados;

4. Propagação de políticas de segurança da informação e proteção de dados a todos os colaboradores e eventuais terceiros contratados que vierem a ter acesso a informações relevantes, bem como a vinculação de tais colaboradores e terceiros à obrigações específicas neste sentido;

5. Manutenção de ambiente de segurança resiliente para o tratamento das informações relacionadas ao Contrato, bem como da realização de avaliações técnicas periódicas (ao menos anualmente) para a avaliação da resiliência do ambiente de tecnologia e gestão de vulnerabilidades em seus sistemas e demais estruturas físicas e digitais, sobretudo a fim de prevenir Incidentes, incluindo testes de penetração, aplicando todas as medidas técnicas e de governança comumente utilizadas pelo mercado e que sejam cabíveis para mitigar os riscos detectados;

6. Aplicação das metodologias de *Privacy by Design* e *Security by Design* na execução de suas atividades no âmbito do Contrato, em especial no desenvolvimento, atualização e utilização de tecnologias necessárias ao cumprimento de suas obrigações contratuais;

7. Implementação de medidas técnicas e de governança dedicadas a:

7.1 Negar o acesso de pessoas não autorizadas aos equipamentos e demais estruturas utilizadas para o tratamento de informações relacionadas ao Contrato;
7.2 Impedir a leitura, entrada, cópia, modificação, inspeção ou eliminação não autorizada de informações por pessoas não autorizadas; inclusive para casos de transferência dos dados e fins de armazenamento físico ou eletrônico;
7.3 Garantir que apenas os colaboradores autorizados a utilizar sistemas informacionais tenham acesso às informações cobertas pela sua autorização de acesso;
7.4 Assegurar que é possível verificar e estabelecer para quais indivíduos as informações foram ou podem ser transmitidas, disponibilizadas, compartilhadas ou transferidas utilizando equipamentos de comunicação;

7.5 Assegurar a possibilidade de identificar a entrada e o fluxo de informações em sistemas;

7.6 Garantir que os sistemas utilizados para o tratamento de informações relacionadas ao Contrato, em caso de interrupção, possam ser restaurados em tempo razoável, sem que os dados sejam corrompidos, alterados ou completamente indisponibilizados em razão do mau funcionamento dos sistemas;

7.7 Garantir o monitoramento contínuo dos sistemas e medidas técnicas de segurança da informação;

7.8 Assegurar que os processos de gerenciamento de risco da cadeia de suprimentos cibernéticos sejam identificados, estabelecidos, avaliados, gerenciados e acordados por partes;

7.9 Assegurar que fornecedores e parceiros terceirizados de sistemas de informação, componentes e serviços sejam identificados e avaliados por meio de um processo de avaliação de risco da cadeia de suprimentos cibernéticos;

7.10 Garantir que os contratos com fornecedores e parceiros terceirizados sejam usados para implementar medidas adequadas projetadas para atender aos objetivos do programa de segurança cibernética das partes;

7.11 Fornecedores e parceiros terceirizados sejam avaliados periodicamente usando auditorias, resultados de testes ou outras formas de avaliações para confirmar que estão cumprindo suas obrigações contratuais;

7.12 Planejamento e testes de resposta e recuperação sejam realizados com fornecedores e provedores terceirizados;

8. Avaliação prévia por profissionais com conhecimento quanto aos impactos potenciais de qualquer mudança de processo, controle e demais medidas relacionadas à segurança da informação e proteção de dados;

9. Emprego de recursos humanos suficientes para garantir a atuação de equipe (própria ou terceirizada) responsável pelos controles, políticas e demais medidas relacionadas à segurança da informação, especialmente para detecção de e resposta a incidentes, gestão de impacto e resolução de ocorrências, com regime de cobertura perene, acessível 24 (vinte e quatro) horas por dia, 7 dias por semana;

10. Implementação de proteções adequadas para que informações em qualquer formato estejam seguras e protegidas contra incidentes, dentre os quais decorrentes de desastre naturais e riscos ambientais;

11. Utilização de soluções tais como encriptação de dados nos ativos de informação utilizados pelos colaboradores e terceiros contratados, inclusive em recursos de tecnologia móveis, tal como notebooks, aparelhos celulares e demais dispositivos onde são armazenadas informações;

12. Realização de procedimentos de backup e recuperação de dados com frequência adequada ao contrato, de forma a garantir o cumprimento dos requisitos de proteção e restauração de dados;

13. Informações armazenadas em mídias removíveis sejam protegidas contra incidentes, incluindo, mas não se limitando à restrição de funcionalidades de uso de mídias removíveis para prevenir leitura, cópia, modificação, extração ou eliminação não autorizada de dados;

14. Implementação de medidas e controles para detectar e prevenir a inserção, a extração, a modificação a eliminação ou qualquer forma de tratamento indevido de informações relacionadas ao Contrato, inclusive por meio da utilização de firewalls e softwares antivírus atualizados, da adoção de soluções tais como *Data Loss Prevention* (*DLP*), bem como proteção contra malware e outros programas maliciosos;

15. Implementação de medidas para garantir que seja possível verificar quais informações foram inseridas, acessadas, modificadas ou eliminadas nos sistemas e ambientes utilizados, de forma a permitir a identificação dos indivíduos responsáveis pelas ações em questão, bem como a data e o horário de tais ações;

16. Deverá ser realizada a manutenção dos registros (logs) pertinentes às obrigações da CONTRATADA, protegidos e retidos durante o período de vigência contratual, e por pelo menos 6 (seis) meses a contar do término do Contrato, inclusive para que possam ser objeto de análise forense, caso necessário à apuração de incidentes;

17. No que se refere à tomada de medidas necessárias à cooperação com a CONTRATANTE, no âmbito do contrato e das diretrizes e legislações aplicáveis, a CONTRATADA se compromete a utilizar sistemas capazes de viabilizar o cumprimento de suas obrigações;

18. Estabelecimento e implementação de procedimento documentado para a gestão de incidentes de qualquer natureza, com a capacitação e treinamento de todos os indivíduos envolvidos no uso de informações relacionadas ao Contrato, com o envio de informações comprobatórias à CONTRATANTE no que a ela impactar, quando solicitado;

19. Mediante solicitação, e em prazo acordado entre as partes, a CONTRATADA deverá apresentar à CONTRATANTE evidências de implementação das medidas e controles relativos à segurança da informação.