

Condições Especiais de Compra

Anexo - Segurança da Informação

Estas Condições Especiais de Compra são parte integrante das Condições Gerais de Compra (“CGC”) que regulam o fornecimento de Mercadorias e/ou Serviços entre a Mercedes-Benz do Brasil Ltda. (“MBBRAS”) e o Fornecedor destinatário da contratação, relativas à segurança das informações, definindo os padrões e critérios que os Fornecedores devem cumprir para garantir o objetivo comum de segurança das informações da MBBRAS e/ou do Fornecedor.

Capítulo I – Segurança da Informação

1. Manuseio seguro de informações e proteção de sistemas

Para garantir a confidencialidade, a integridade e disponibilidade das informações compartilhadas pela MBBRAS, as partes contratantes comprometem-se a proteger efetivamente todas as informações compartilhadas contra acesso não autorizado, modificação, destruição ou perda, transmissão não autorizada, outros processamentos não autorizados e outros usos indevidos, de acordo com o estado atual da arte.

O Fornecedor deverá tomar medidas preventivas razoáveis para evitar que seus sistemas e ativos criem ameaças à segurança que possam afetar a infraestrutura da MBBRAS, em particular, garantindo que os sistemas e dispositivos de computador relevantes do Fornecedor estejam livres de malware (por exemplo, ransomware).

2. Gerenciamento de incidentes

2.1. Notificação de incidentes

Caso a MBBRAS ou o Fornecedor venha a tomar conhecimento de incidentes que envolvam uma violação de segurança das informações e/ou que coloquem em risco a confidencialidade, a integridade ou a disponibilidade das informações da MBBRAS em sua posse, na medida em que se trate de informações da MBBRAS e/ou possam afetar negativamente a MBBRAS, ou caso existam indicações para a MBBRAS ou Fornecedor que justifiquem a suspeita de tais incidentes de segurança da informação, levando em conta uma avaliação razoável, o Fornecedor deverá, sem qualquer atraso injustificado, notificar a MBBRAS. Isso inclui casos como perda de dados, uso indevido de dados, infecções por malware, acesso não autorizado a informações da MBBRAS (por exemplo, ataque cibernético), vulnerabilidades, outras ameaças de segurança ou se houver quaisquer outras circunstâncias que possam afetar a MBBRAS.

2.2. Pessoa responsável

O Fornecedor deverá nomear pessoas de contato responsáveis pela segurança das informações, que são responsáveis por comunicar incidentes e violações de segurança à MBBRAS, bem como monitorar a resposta e as medidas corretivas.

2.3. Medidas corretivas de incidentes

O Fornecedor deverá garantir que tais incidentes, violações de segurança da informação e vulnerabilidades críticas sejam resolvidas sem atrasos indevidos e sem cobrança adicional. Imediatamente após tomar conhecimento do incidente de segurança, o Fornecedor se compromete a fornecer todo o suporte necessário à MBBRAS, incluindo medidas de mitigação e sua implantação, cumprindo com os prazos indicados neste Anexo para mitigar os danos e apoiar a MBBRAS na restauração das informações. A pedido do MBBRAS, o Fornecedor enviará um relatório detalhado do incidente e deverá incluir os resultados dos testes de segurança, riscos de segurança da informação identificados e incidentes de segurança da informação identificados, e medidas adotadas ou a serem adotadas.

O Fornecedor se compromete a manter um plano de contingência para os serviços contratados, que deverá conter planos detalhados de continuidade do negócio e recuperação do negócio em caso de Incidente de Segurança.

3. Conscientização da equipe

Caso o Fornecedor tenha acesso a ferramentas de processamento de dados da MBBRAS ou utilizadas pela MBBRAS, eventual concessão do acesso a pessoas não autorizadas somente será permitida mediante aprovação prévia da MBBRAS, para uso dentro do escopo necessário para a execução do contrato. O Fornecedor deve, ainda, manter seus funcionários, subcontratados e outras pessoas envolvidas na prestação dos serviços, com acesso ou privilégios de acessos a tais ferramentas sobre as diretrizes de segurança da informação e os procedimentos específicos como, por exemplo, o gerenciamento de incidentes com relação a esse acesso, incluindo as limitações de uso das informações do MBBRAS.

4. Certificação de segurança da informação

Dependendo do tipo e dos requisitos de proteção das informações da MBBRAS em questão ou da importância dos serviços do Fornecedor para as operações comerciais da MBBRAS, a MBBRAS pode exigir que o Fornecedor adote um nível apropriado de medidas de segurança para a segurança das informações durante toda a relação comercial. O Fornecedor deverá fornecer evidências de um nível adequado de segurança das informações nas instalações do Fornecedor, em particular, apresentando o selo TISAX® com Nível de Avaliação 3 para fornecedores de material de produção. A MBBRAS pode solicitar o mesmo selo de todos os outros

fornecedores dentro do respectivo contrato. As partes podem acordar um período razoável para o teste inicial de um local de acordo com o respectivo certificado e/ou quaisquer alterações de requisitos no nível apropriado de segurança das informações.

5. Direito de inspeção

Se a MBBRAS tomar conhecimento de uma violação da implementação e manutenção dos requisitos de segurança da informação acordados, da existência de um incidente de segurança da informação ou se houver indícios razoáveis para suspeitar de tal violação, a MBBRAS terá o direito de verificar a conformidade com os requisitos de segurança da informação e os requisitos adicionais de segurança da informação acordados ("Auditorias"). O Fornecedor cooperará para fornecer as informações necessárias, na medida exigida para a Auditoria. A MBBRAS poderá, após notificação oportuna, durante o horário comercial normal e, na medida do possível e razoável, também inspecionar as instalações do Fornecedor, incluindo os sistemas de TI relevantes, para verificar a conformidade com as medidas técnicas e organizacionais acordadas sem interromper os processos operacionais. Ao fazê-lo, a MBBRAS deverá observar quaisquer obrigações de confidencialidade do Fornecedor para com terceiros. A MBBRAS terá o direito de fazer com que as auditorias sejam realizadas por uma empresa externa e qualificada que esteja vinculada à confidencialidade em relação a terceiros, desde que essa empresa não seja concorrente do Fornecedor. Isso não restringirá nem excluirá o direito de inspeção e informação da MBBRAS.

Capítulo II - Prestação de Serviços de Automação, Aquisição e Modificação de Máquinas e Equipamentos

6. Aplicação Específica

Sem prejuízo das disposições acima, aplicáveis a todas as contratações, nos casos específicos de prestação de serviços de automação, aquisição e modificação de máquinas e equipamentos, aplicam-se, adicionalmente, as disposições deste Capítulo II.

7. Treinamento

Anualmente, a MBBRAS fornecerá treinamento ao Fornecedor sobre diretivas relativas à segurança da informação aplicáveis ao Contrato, devendo o Fornecedor manifestar formalmente por meio da assinatura de documento próprio, ciência do conteúdo ministrado e seu cumprimento integral. Em caso de recusa do Fornecedor em participar do treinamento ou submeter-se às normas da MBBRAS relativas à segurança da informação, os serviços ou contratação serão suspensos, bem como o respectivo pagamento. O descumprimento injustificado das diretivas informadas pela MBBRAS poderá causar a rescisão justificada e antecipada do contrato de prestação de serviços.

8. Correção de Vulnerabilidades

8.1. O Fornecedor é responsável por corrigir quaisquer vulnerabilidades de segurança cibernética identificadas nos equipamentos fornecidos à MBBRAS. Em caso de compra de equipamentos de empresa terceira, o Fornecedor será responsável pelo trâmite de cobrança e cumprimento do SLA pela empresa terceira.

8.1.1 A correção de vulnerabilidades deve ser realizada de acordo com as melhores práticas da indústria e com a máxima urgência para mitigar qualquer risco para a segurança da MBBRAS.

8.1.2 Em caso de necessidade de correção de vulnerabilidade, o Fornecedor deverá:

- (i) Fornecer à MBBRAS uma descrição detalhada do método de correção para cada vulnerabilidade identificada, que deverá conter instruções e passo a passo para implementação da correção e quaisquer ferramentas adicionais necessárias;
- (ii) Lançar uma correção para a vulnerabilidade em prazo de acordo com a classificação de risco da vulnerabilidade: se crítica, 1 (um) mês; se alta 2 (dois) meses; e se baixa 3 (três) meses, contados da data de identificação da vulnerabilidade. A análise de risco será feita pela MBBRAS por meio de ferramenta específica de identificação de vulnerabilidades de segurança cibernética.

8.1.3. Em caso de descumprimento do prazo estabelecido no item (ii) da Cláusula 8.1.2. ou falha na correção da vulnerabilidade, durante o período em que as informações e sistemas da MBBRAS ficarem expostas ao risco decorrente da vulnerabilidade, o Fornecedor será responsável por auxiliar a MBBRAS na recuperação do ambiente afetado e por quaisquer danos causados à MBBRAS, incluindo, mas não se limitando àqueles provenientes de ataques cibernéticos aos sistemas ou equipamentos contratados, ressaltando-se à MBBRAS o direito de adotar medidas adequadas para proteção de sua infraestrutura.