POLÍTICA DE SEGURANÇA CIBERNÉTICA - FORNECEDORES

OBJETIVO

O objetivo desta política é comunicar as considerações gerais de segurança da informação estabelecidas pelo Mercado Pago e Mercado Crédito aos terceiros afetados por ela. Os terceiros envolvidos estarão cientes das referidas diretrizes de segurança e assumirão o compromisso de realizar todos os esforços razoáveis para cumprir esta política.

APLICAÇÃO

Esta política é aplicável para terceiros que prestam serviços, parceiros comerciais e integradores que acessam, consomem e/ou processam dados e/ou têm acesso e interação com sistemas e infraestrutura tecnológica do Mercado Pago e Mercado Crédito.

Os terceiros são classificados de acordo com seu nível de criticidade, estrutura regulatória e seu impacto potencial sobre a confidencialidade, disponibilidade ou integridade da informação e infraestrutura tecnológica dentro da estrutura do objeto do contrato pré-estabelecido e assinado entre as partes.

DEFINIÇÕES

Para os fins desta política, aplicam-se as seguintes definições:

- **Instituição:** Refere-se às entidades Mercado Pago e Mercado Crédito.
- **Fornecedores e Terceiros:** Empresas com as quais a instituição mantém relação comercial, através da qual são fornecidos ou recebidos produtos e/ou serviços.
- **Assessment de segurança:** Questionário elaborado pela Área de Segurança da Informação, baseado em frameworks e melhores práticas de mercado em Segurança da Informação.
- **Colaboradores:** funcionários efetivos e/ou terceirizados da instituição.
- **Incidente de Segurança:** refere-se a: (i) qualquer descumprimento (incluindo, mas não se limitando a, descumprimento do Serviço) detectado nas instalações, equipamentos, sistemas ou pessoas contratadas ou empregadas pelo FORNECEDOR (doravante um

"Descumprimento"), que poderia razoavelmente esperar-se que tenha um efeito adverso na segurança, confidencialidade ou integridade dos Dados e dos sistemas envolvidos; (ii) qualquer apropriação de Dados e/ou situação que implique ou constitua um Uso não autorizado ou alteração dos Dados e dos sistemas e/ou servidores envolvidos; bem como qualquer situação que implique uma afetação à sua segurança ou constitua uma Utilização não autorizada dos Dados e (iii) qualquer descumprimento da Política de Segurança da Informação e/ou do Regulamento relativo à Proteção de Dados.

- **Segurança Informação:** processo para proteger os recursos informáticos da organização nos seus pilares de confidencialidade, integridade, disponibilidade e rastreabilidade.
- **Usuários:** pessoas físicas que utilizam os produtos e/ou serviços da instituição.

DIRETRIZES

PRINCÍPIOS CORPORATIVOS

A instituição busca democratizar o comércio eletrônico e desenvolver produtos de forma segura, sempre com o objetivo de proteger as informações e os dados confidenciais dos usuários e/ou colaboradores.

Os elementos de Segurança da informação são considerados fatores-chave para mitigar riscos e promover o cumprimento das leis de privacidade e proteção financeira dos Usuários. Na mesma linha, buscamos proteger os dados e informações que os terceiros possuem ou processam; com base nas melhores práticas como ISO, NIST, PCI, etc.

GESTÃO DE TERCEIROS

Para garantir a gestão adequada de terceiros, a instituição estabelece controles, tanto técnicos quanto legais, para minimizar o impacto de um incidente gerado por um terceiro relacionado. Dessa forma, adotamos cláusulas legais que exigem controles mínimos razoáveis que garantam a proteção

dos dados e dos ativos que são acessados. Neste sentido, o terceiro reconhece, compreende e compromete-se a fazer todos os esforços razoáveis para cumprir esta política.

AVALIAÇÃO DE SEGURANÇA DE TERCEIROS

A instituição possui um processo de avaliação de riscos de Segurança Informática que aplica para todos os terceiros aplicáveis. O terceiro pode ser avaliado pela instituição por meio de um questionário de Assessment de segurança elaborado pela Área de Segurança da Informação, que contempla frameworks e melhores práticas do setor sobre segurança da informação.

Durante o processo de avaliação e ao ser notificada sobre mudanças na região de prestação de serviço, a instituição verificará se existe convênio entre o BACEN e as autoridades supervisoras dos países onde os serviços poderão ser prestados e diante da inexistência de convênio a instituição solicitará autorização do Banco Central do Brasil com antecedência de 60 dias para que possa firmar contrato.

GESTÃO DE INCIDENTES DE SEGURANÇA

O terceiro deve ter um processo definido e formalizado para responder a incidentes de segurança. Os incidentes devem ser identificados, classificados, monitorados, comunicados e devidamente tratados de forma a reduzir os riscos no ambiente de segurança, evitando a interrupção das atividades ou defeitos em sua operação ou a afetação da confidencialidade, integridade e disponibilidade dos ativos de informação da instituição.

RECOMENDAÇÕES DE SEGURANÇA PARA O TERCEIRO

O terceiro deve manter um programa de Segurança da Informação que contenha informações administrativas e técnicas para salvaguardar os dados e/ou sistemas, infraestrutura e processos da instituição aos quais o terceiro tenha acesso e/ou interação. Este programa deve ser adequado às complexidades da natureza e escopo de suas atividades e à sensibilidade de seus ativos de informação.

Essas salvaguardas devem incluir, pelo menos, entre outros, os seguintes:

POLÍTICA DE SEGURANÇA CIBERNÉTICA - FORNECEDORES

1. Ter uma área de governança e segurança da informação que estabeleça as diretrizes gerais de segurança da informação para garantir um ambiente de segurança adequado.

2. Proteger contra ameaças ou perigos previstos a segurança ou integridade, informações, sistemas, infraestrutura e processos da instituição.

3. Proteger contra o acesso ou uso não autorizado de informações da instituição que possam resultar em danos ou inconvenientes substanciais para nossos usuários e/ou colaboradores, bem como outras entidades.

4. Assegurar a existência de um programa anual de treinamento e conscientização em Segurança da Informação para todos os colaboradores, bem como terceiros com acesso ao seu ambiente.

5. Ter processos e controles formalmente definidos com o objetivo de prevenir, detectar e reduzir vulnerabilidades relacionadas ao ambiente cibernético que abranjam, no mínimo, a autenticação, a criptografia, a prevenção e o gerenciamento de intrusões indesejadas, a proteção de informações, a realização periódica de testes e scans para a detecção de vulnerabilidades, a proteção contra malware, o estabelecimento de logs, os controles de acesso e segmentação da rede de computadores e a manutenção de backups dos dados.

6. Definir e manter um programa de continuidade de negócios e gestão e resposta a incidentes para minimizar o impacto na prestação de serviços e/ou relações comerciais estratégicas à instituição em caso de possíveis incidentes que possam afetar a continuidade das operações.

7. Definir e manter um processo de gerenciamento de dados e backups, a fim de evitar ou mitigar a perda de dados em caso de incidentes.

8. Possuir mecanismos de monitoramento dos serviços prestados e/ou processos-chave em relação à instituição.

POLÍTICA DE SEGURANÇA CIBERNÉTICA - FORNECEDORES

9. Contar com um procedimento de identificação e segregação dos dados armazenados e/ou processados da instituição por meio de controles físicos e lógicos.

10. Ter um processo de desenvolvimento seguro, quando aplicável, alinhado às melhores práticas, como OWASP Top 10.

11. Se aplicável, contar com procedimentos para transmissão das informações sobre as operações realizadas, a partir do terminal até a plataforma tecnológica do Mercado Pago, utilizando mecanismos de criptografia fortes.

12. Se aplicável, zelar para que as informações enviadas aos clientes estejam livres de software malicioso.

13. Se aplicável, definir e manter campanhas de informação sobre as medidas de segurança que os clientes devem adotar para a realização de operações de comércio eletrônico. Aplica-se a estabelecimentos comerciais ou entidades administradoras de gateways de pagamento.

14. Utilizar as credenciais de acesso fornecidas pela instituição e apenas para acessar as plataformas e/ou sistemas da instituição.

15. Se aplicável, para o relacionamento com terceiros correspondentes da instituição, também é preciso:
    - Contar com mecanismos e/ou procedimentos que impeçam a captura, armazenamento, processamento, visualização ou transmissão da informação das operações realizadas, para fins diferentes dos autorizados pela instituição.
    - Da mesma forma, operar com sistemas de informação que permitam que as operações sejam realizadas em condições de segurança, qualidade e não repúdio pelo correspondente.