POLÍTICA DE SEGURANÇA CIBERNÉTICA - FORNECEDORES

OBJETIVO

A presente política com o principal objetivo de orientar e direcionar nossos fornecedores acerca de Processos e Controles de Segurança da Informação necessários para garantir a Confidencialidade, Disponibilidade e Integridade das informações da Instituição, aumentando assim a proteção das informações manuseadas, processadas e/ou armazenadas pelo fornecedor. Trata-se de uma extensão da política interna de Segurança Cibernética com os principais pontos focados em fornecedores.

APLICAÇÃO

Esta política é aplicável a todos os fornecedores que prestem serviços ou gerem impacto direto, como prestadores de serviços, terceiros, parceiros de negócio e integradores que consomem ou processam dados.

O fornecedor designará indivíduos ou equipes nomeados que terão responsabilidade pela política, implementação e processos de segurança da informação. Tais indivíduos nomeados devem atuar com os principais pontos de contato da Instituição, para atividades de Segurança da Informação. Além disso, devem facilitar qualquer revisão da área de segurança, reuniões e gerenciar qualquer plano de restauração em caso de violação da segurança das informações.

DEFINIÇÕES

Para fins desta Política, são aplicáveis as seguintes definições:

- **BACEN**: Banco Central do Brasil.
- **Fornecedores:** Empresas contratadas pela Instituição para a prestação de serviços.
- **Fornecedores Relevantes:** Empresas contratadas para prestação de serviços que se enquadram em critérios específicos contidos neste documento.
- **Checklist:** Questionário elaborado pela Área de Segurança da Informação, com base em frameworks e melhores práticas de mercado.

POLÍTICA DE SEGURANÇA CIBERNÉTICA - FORNECEDORES

- **Mercado Pago:** MercadoPago.Com Representações Ltda.
- **Mercado Crédito SCFI:** Mercado Crédito Sociedade de Crédito Financiamento e Investimento S.A.
- **Instituição:** Refere-se às entidades Mercado Livre, Mercado Pago e Mercado Crédito SCFI.

DIRETRIZES

PRINCÍPIOS

Os elementos de Segurança Cibernética são considerados fatores chaves para mitigar os riscos e promover o cumprimento das leis de privacidade e proteção financeira do cliente. Em linha buscamos zelar com os mesmos cuidados os dados e informações que trafegam e/ou são armazenados em bases de dados terceirizadas.

GESTÃO DE TERCEIROS

Para garantir a devida gestão de terceiros a Instituição estabelecem controles, tanto técnicos como legais, para minimizar o impacto de um incidente gerado por um parceiro comercial. Desta forma, adotamos cláusulas legais de obrigatoriedade de existência de controles mínimos razoáveis que garantam a proteção dos dados e dos dos ativos de Tecnologia acessados. Além de cláusulas de Privacidade e Proteção de Dados Pessoais, em conformidade com a Lei Geral de Proteção de Dados Pessoais.

GESTÃO DE INCIDENTES DE SEGURANÇA

O fornecedor deve possuir um processo de Resposta a Incidentes. Os incidentes de segurança devem ser identificados, monitorados, comunicados e devidamente tratados de forma a reduzir riscos no ambiente, evitando interrupção das atividades.

Comunicação de Incidentes

Caso seja detectado algum incidente de segurança cibernética de impacto crítico, ou seja, que possa causar indisponibilidade nos serviços e/ou na operação, infraestrutura tecnológica e gerar uma crise

ou demais situações em que um incidente de Segurança da Informação envolve acesso ou comprometimento de informações da Instituição, solicitamos:

- Comunicar **imediatamente** a caixa de e-mail **irsec@mercadolibre.com** e notificar a equipe de Segurança da Informação, assim tomaremos as medidas necessárias para detecção, mitigação e respostas internamente.
- Efetuar as medidas de contenção e resposta ao incidente de forma coordenada com a equipe de Segurança da Informação da Instituição, participando das ações de remediação e crise em conjunto entre as equipes.

No caso de confirmação de um incidente envolvendo dados pelos quais a Instituição seja responsável, deverá ser avaliado em conjunto se as ações realizadas na fase de remediação estão de acordo com os padrões de Segurança da Instituição.

Além disso, quando o incidente impactar o Ambiente Mercado Pago e Mercado Crédito, a área de Segurança da Informação deverá notificar o Bacen sobre o Incidente ocorrido no Fornecedor.

FORNECEDORES RELEVANTES

A Instituição possui regras de diligência para contratação de fornecedores considerados relevantes. Segue abaixo critérios que indicam que o fornecedor deve ser avaliado por Segurança da Informação por se tratar de um serviço relevante:

- Fornecedor armazena, processa e/ou consome dados sensíveis de clientes da Instituição, em On Premise/Cloud;
- Fornecedor tem acesso a infraestrutura ou sistemas de informação da Instituição;
- Fornecedor provê serviços que podem gerar alto impacto nos negócios ou que possa comprometer a disponibilidade, integridade, confidencialidade das informações da Instituição; e
- Fornecedor possui impacto alto em volume de transações financeiras (% TPV, GMV).

POLÍTICA DE SEGURANÇA CIBERNÉTICA - FORNECEDORES

Além dos critérios acima, caso a Área de Segurança da Informação verifique necessidade, ela poderá avaliar demais fornecedores que não se encaixem nos critérios acima.

AVALIAÇÃO DE FORNECEDOR RELEVANTE

Antes da contratação os fornecedores devem ser avaliados por meio de um "Checklist" elaborado pela Área de Segurança da Informação, considerando frameworks e melhores práticas de mercado.

Ele deverá ser preenchido pelo fornecedor e avaliado por Segurança da Informação. Caso considere necessário, a área de Segurança poderá solicitar evidências bem como a validação presencial de processos e controles do fornecedor.

Para os fornecedores já contratados até a data de publicação dessa política, a Instituição poderá fazer, caso identifique ser necessário, avaliações referentes aos controles de Segurança da Informação e demais controles que julgar necessário do fornecedor.

SUBCONTRATAÇÃO DE SERVIÇOS

Havendo necessidade de subcontratação de serviços relevantes, o fornecedor deverá realizar notificação de imediato a equipe de Segurança da Informação da Instituição.

Caso os serviços sejam de processamento e armazenamento de dados e de computação em nuvem, e sejam referentes ao ambiente do Mercado Pago e Mercado Crédito, deve-se observar, se os serviços são prestados em localidades primárias no exterior, deve-se observar a existência de convênio entre o BACEN e as autoridades supervisoras dos países onde os serviços poderão ser prestados, devendo assegurar que a prestação dos referidos serviços não cause prejuízos ao seu funcionamento, nem embaraço à atuação do BACEN.

REQUISITOS DE SEGURANÇA PARA O FORNECEDOR

O Fornecedor deverá manter um abrangente Programa de Segurança da Informação que contém informações administrativas, técnicas e físicas para salvaguardar as informações, adequadas à complexidade, natureza e escopo de suas atividades e à sensibilidade de seus ativos de informação.

Tais salvaguardas deverão incluir os elementos estabelecidos abaixo:

POLÍTICA DE SEGURANÇA CIBERNÉTICA - FORNECEDORES

- Alcançar a segurança e a confidencialidade das informações da Instituição;
- Proteger contra ameaças ou perigos previstos à segurança ou integridade das Informações da Instituição;
- Proteger contra acesso não autorizado ou uso de Informações da Instituição em que possam resultar em danos substanciais ou inconveniente para a Instituição e suas empresas bem como seus clientes e / ou consumidores,
- Fornecer documentação de forma periódica (anual) que comprovem as certificações apresentadas, bem como apresentar resultados de diligência interna quanto à eficácia contínua dos controles;
- Permitir auditoria e análise, previamente acordada, referente ao funcionamento da operação e dos controles apresentados;
- Assegurar da existência de um programa anual de treinamento e conscientização em Segurança da Informação e Privacidade para todos os colaboradores, bem como a seus terceiros alocados no ambiente;
- Possuir Processos e Controles com o objetivo de prevenir, detectar e reduzir vulnerabilidades relacionadas com o ambiente cibernético, abrangendo autenticação, criptografia, prevenção e a detecção de intrusão, a prevenção de vazamento de informações, a realização periódica de testes e varreduras para detecção de vulnerabilidade, a proteção contra softwares maliciosos, o estabelecimento de mecanismos de rastreabilidade, os controles de acesso e de segmentação da rede de computadores e a manutenção de cópias de segurança dos dados e das informações;
- Definir e manter um programa de Privacidade de Dados Pessoais, de acordo com a Lei Geral de Proteção de Dados Pessoais, além de tratar os dados pessoais conforme as orientações da Instituição, quando esse for Controlador;
- Definir e manter um programa de continuidade de negócios para minimizar os impactos na prestação de serviços da Instituição em caso de possíveis incidentes;

- Definir e manter um processo de gestão e retenção de dados (Backups), de forma a evitar ou mitigar a perda de dados diante de incidentes;
- Possuir mecanismos para o monitoramento dos serviços prestados;
- Permitir o acesso da Instituição, caso necessário, aos relatórios elaborados por empresas de auditorias externas, relativos aos procedimentos e aos controles utilizados na prestação dos serviços a contratados;
- Prover, se necessário, documentação que comprove a identificação e a segregação dos dados armazenados/processados da Instituição por meio de controles físicos e/ou lógicos; e
- Possuir Processo de Desenvolvimento Seguro.

RESPONSABILIDADES

Segurança da Informação

- Responsável por efetuar a avaliação de risco dos fornecedores;
- Responsável por encaminhar o" Checklist" de Avaliação para o fornecedor;
- Responsável por avaliar o fornecedor com base nas respostas do checklist e em casos onde avalie a necessidade, solicitar documentos adicionais e realizar visitas in loco;
- Responsável por identificar se o fornecedor possui controles suficientes para cumprir a Confidencialidade, Integridade e Disponibilidade das informações da Instituição;

Fornecedores

- Responsável por informar a Instituição caso ocorra incidente crítico ou indisponibilidade do seu ambiente através dos meios informados nesta política.
- Responsável por responder o "Checklist" de Segurança da Informação com informações verídicas.

POLÍTICA DE SEGURANÇA CIBERNÉTICA - FORNECEDORES

- Responsável por atender in loco a equipe de Segurança da Informação re-validando informações preenchidas no "Checklist", caso seja necessário.
- Responsável por fornecer evidências e documentos que suportem as informações fornecidas no questionário, quando solicitadas.
- Responsável por notificar a área de Segurança da Informação da Instituição caso haja alterações relevantes no seu ambiente.