Sumário

1. Introdução e Apresentação da OMID Solutions

A OMID Solutions é uma empresa especializada na prestação de serviços de tecnologia de alta qualidade, oferecendo soluções em colocation de recursos físicos e cloud corporativa de alto desempenho definida por software. Nossa organização também disponibiliza serviços especializados como certificação digital, consultoria tecnológica, gerenciamento de infraestrutura, monitoramento de sistemas e soluções de armazenamento de dados.

Nossa missão é proporcionar aos nossos clientes uma infraestrutura de cloud segura, flexível e facilmente escalável, que funcione de maneira transparente, utilizando tecnologia familiar, inteligente e com total previsibilidade de custos. Para alcançar este objetivo, mantemos os mais altos padrões de segurança da informação em todos os aspectos de nossas operações.

A segurança da informação é um pilar fundamental de nossos serviços e operações. Reconhecemos que a confiança de nossos clientes depende diretamente de nossa capacidade de proteger suas informações e ativos digitais com o máximo rigor e eficiência. Por esta razão, estabelecemos diretrizes rigorosas de segurança que se estendem não apenas às nossas operações internas, mas também a todos os nossos parceiros comerciais, fornecedores e prestadores de serviços.

Esta política representa nosso compromisso com a excelência em segurança da informação e estabelece as expectativas claras que temos em relação aos nossos fornecedores e parceiros. Através da implementação consistente destes padrões, garantimos que toda a cadeia de valor mantenha o mesmo nível de proteção e confidencialidade que nossos clientes esperam e merecem.

A proteção adequada das informações não é apenas uma questão técnica, mas também uma responsabilidade ética e legal que assumimos perante nossos clientes, colaboradores e a sociedade. Esperamos que todos os nossos fornecedores compartilhem desta visão e se comprometam com os mesmos padrões de excelência que praticamos internamente.

2. Objetivos desta Política

Esta Política de Segurança da Informação para Fornecedores tem como objetivo principal estabelecer diretrizes claras e abrangentes para garantir que todos os fornecedores, prestadores de serviços e parceiros comerciais da OMID Solutions mantenham padrões adequados de segurança da informação em suas interações conosco.

O primeiro objetivo fundamental é assegurar a proteção integral das informações corporativas da OMID Solutions que possam ser acessadas, processadas, armazenadas ou transmitidas por fornecedores durante a prestação de seus serviços. Isso inclui dados de clientes, informações técnicas, dados operacionais, propriedade intelectual e qualquer outra informação considerada sensível ou confidencial.

Buscamos também estabelecer um framework comum de segurança que permita a integração segura de fornecedores em nossos processos operacionais, garantindo que não haja comprometimento dos controles de segurança estabelecidos internamente. Esta integração deve ser transparente para nossos clientes finais, mantendo a mesma qualidade e segurança que eles esperam de nossos serviços diretos.

Outro objetivo crucial é definir responsabilidades claras e específicas para cada parte envolvida na cadeia de fornecimento, eliminando ambiguidades que possam resultar em falhas de segurança. Cada fornecedor deve compreender exatamente quais são suas obrigações em termos de segurança da informação e como estas se relacionam com nossos objetivos organizacionais mais amplos.

A política também visa estabelecer mecanismos efetivos de monitoramento e auditoria que permitam verificar continuamente o cumprimento dos requisitos de segurança por parte dos fornecedores. Isso inclui a definição de indicadores de desempenho, procedimentos de avaliação e critérios para ações corretivas quando necessário.

Finalmente, objetivamos criar um ambiente de melhoria contínua onde fornecedores sejam incentivados a aprimorar constantemente seus controles de segurança, contribuindo para o fortalecimento geral da postura de segurança de toda a cadeia de valor. Esta abordagem colaborativa beneficia não apenas a OMID Solutions, mas também nossos clientes e os próprios fornecedores.

3. Abrangência e Aplicabilidade

Esta política aplica-se de forma abrangente a todos os fornecedores, prestadores de serviços, consultores, parceiros comerciais e terceiros que tenham qualquer forma de relacionamento comercial ou operacional com a OMID Solutions. A aplicabilidade não se limita apenas aos contratos principais, mas estende-se também a subcontratados e parceiros dos fornecedores que possam ter acesso direto ou indireto às informações da OMID Solutions.

A política é aplicável independentemente da natureza do serviço prestado, seja ele relacionado a tecnologia da informação, serviços administrativos, manutenção, consultoria, suporte técnico ou qualquer outra atividade que

envolva o manuseio de informações corporativas. Todos os fornecedores devem aderir a estas diretrizes desde o momento da contratação até o encerramento completo do relacionamento comercial.

O escopo de aplicação inclui todas as formas de acesso a informações da OMID Solutions, seja através de sistemas eletrônicos, documentos físicos, comunicações verbais ou qualquer outro meio. Isso abrange situações onde fornecedores trabalham em nossas instalações, remotamente, ou em suas próprias dependências, desde que estejam manuseando informações de nossa propriedade.

A política também se aplica a todas as fases do ciclo de vida da informação, incluindo coleta, processamento, armazenamento, transmissão, compartilhamento e descarte seguro. Fornecedores devem garantir que controles adequados sejam implementados em cada uma destas fases, independentemente da tecnologia ou processo utilizado.

É importante destacar que a aplicabilidade desta política não se limita ao período de vigência dos contratos formais. Certas obrigações, particularmente aquelas relacionadas à confidencialidade e ao descarte seguro de informações, permanecem válidas mesmo após o término do relacionamento comercial, conforme especificado nos acordos contratuais específicos.

A OMID Solutions reserva-se o direito de aplicar esta política de forma diferenciada com base no nível de criticidade das informações envolvidas e no tipo de acesso requerido pelo fornecedor. Fornecedores que lidam com informações mais sensíveis ou que possuem acesso privilegiado podem estar sujeitos a requisitos adicionais de segurança.

4. Princípios Fundamentais de Segurança da Informação

A segurança da informação na OMID Solutions baseia-se em três pilares fundamentais que devem ser rigorosamente observados por todos os fornecedores em suas operações e interações conosco. Estes princípios constituem a base conceitual sobre a qual todos os controles e procedimentos de segurança são construídos.

4.1 Confidencialidade

O princípio da confidencialidade garante que as informações sejam acessíveis somente às pessoas autorizadas e pelo período estritamente necessário para o cumprimento de suas funções. Para os fornecedores, isso significa implementar controles rigorosos de acesso que assegurem que apenas indivíduos

devidamente autorizados e com necessidade legítima de conhecimento possam acessar informações da OMID Solutions.

A confidencialidade deve ser mantida durante todo o ciclo de vida da informação, desde o momento do primeiro acesso até o descarte final. Fornecedores devem implementar medidas técnicas e administrativas que previnam a divulgação não autorizada, seja ela intencional ou acidental. Isso inclui a proteção contra vazamentos através de canais eletrônicos, documentos físicos, conversas informais ou qualquer outro meio de comunicação.

É fundamental que os fornecedores compreendam que a confidencialidade não se aplica apenas às informações explicitamente marcadas como confidenciais, mas a todas as informações da OMID Solutions às quais tenham acesso. A classificação específica de cada informação será comunicada conforme necessário, mas a presunção deve sempre ser de que toda informação requer proteção adequada.

4.2 Integridade

A integridade assegura que as informações permaneçam completas, precisas e inalteradas durante todo o seu ciclo de vida, exceto quando modificações autorizadas forem realizadas por pessoas devidamente credenciadas. Fornecedores devem implementar controles que detectem e previnam alterações não autorizadas, sejam elas causadas por erro humano, falha de sistema ou ação maliciosa.

A manutenção da integridade requer a implementação de mecanismos de verificação e validação que permitam detectar rapidamente qualquer alteração não autorizada. Isso inclui o uso de checksums, assinaturas digitais, controles de versão e outros mecanismos técnicos apropriados para o tipo de informação sendo processada.

Fornecedores devem também estabelecer procedimentos claros para o tratamento de situações onde a integridade das informações possa ter sido comprometida. Isso inclui a notificação imediata à OMID Solutions, a implementação de medidas de contenção e a participação em investigações para determinar a extensão e as causas do comprometimento.

4.3 Disponibilidade

O princípio da disponibilidade garante que as informações e sistemas estejam acessíveis quando necessário para os processos de negócio da OMID Solutions e seus clientes. Fornecedores devem implementar medidas que assegurem a continuidade dos serviços e a recuperação rápida em caso de interrupções.

A disponibilidade não se refere apenas à prevenção de interrupções, mas também à manutenção de níveis adequados de desempenho que permitam o funcionamento eficiente dos processos dependentes. Fornecedores devem estabelecer acordos de nível de serviço claros e implementar monitoramento contínuo para assegurar o cumprimento destes acordos.

É essencial que fornecedores desenvolvam e mantenham planos de continuidade de negócio e recuperação de desastres que sejam compatíveis com os requisitos da OMID Solutions. Estes planos devem ser testados regularmente e atualizados conforme necessário para refletir mudanças nos processos ou na infraestrutura.

5. Responsabilidades dos Fornecedores

Os fornecedores da OMID Solutions assumem responsabilidades específicas e abrangentes relacionadas à segurança da informação que vão além do simples cumprimento de requisitos contratuais básicos. Estas responsabilidades refletem nosso compromisso compartilhado com a proteção de informações sensíveis e a manutenção da confiança de nossos clientes.

5.1 Responsabilidades Gerais de Segurança

Todo fornecedor deve designar um responsável específico pela segurança da informação dentro de sua organização, que servirá como ponto de contato principal para questões relacionadas à segurança. Este responsável deve possuir autoridade adequada para implementar mudanças necessárias e tomar decisões relacionadas à segurança da informação.

Fornecedores devem manter políticas internas de segurança da informação que sejam compatíveis com os requisitos desta política e que demonstrem um compromisso organizacional com a proteção adequada das informações. Estas políticas devem ser documentadas, comunicadas a todos os colaboradores relevantes e atualizadas regularmente.

É responsabilidade do fornecedor garantir que todos os seus colaboradores que tenham acesso a informações da OMID Solutions recebam treinamento adequado sobre segurança da informação e assinem acordos de confidencialidade apropriados. Este treinamento deve ser renovado periodicamente e adaptado às funções específicas de cada colaborador.

5.2 Gestão de Pessoal e Terceiros

Fornecedores devem implementar procedimentos rigorosos de verificação de antecedentes para todos os colaboradores que terão acesso a informações da

OMID Solutions. O nível de verificação deve ser proporcional à sensibilidade das informações e ao tipo de acesso requerido.

Quando fornecedores utilizarem subcontratados ou terceiros para a prestação de serviços que envolvam informações da OMID Solutions, eles devem garantir que estes terceiros também cumpram todos os requisitos desta política. A responsabilidade pela conformidade dos subcontratados permanece com o fornecedor principal.

Procedimentos claros devem ser estabelecidos para o gerenciamento de mudanças de pessoal, incluindo a revogação imediata de acessos quando colaboradores deixarem a organização ou mudarem de função. Fornecedores devem manter registros atualizados de todos os indivíduos com acesso a informações da OMID Solutions.

5.3 Proteção de Informações em Trânsito e em Repouso

Fornecedores são responsáveis por implementar criptografia adequada para proteger informações da OMID Solutions durante a transmissão através de redes públicas ou privadas. Os algoritmos e protocolos de criptografia utilizados devem estar em conformidade com padrões reconhecidos internacionalmente e ser aprovados pela OMID Solutions.

Informações armazenadas em sistemas do fornecedor devem ser protegidas através de controles de acesso apropriados, criptografia quando necessário, e medidas de proteção física adequadas. Fornecedores devem implementar segregação adequada entre informações de diferentes clientes e entre informações de diferentes níveis de sensibilidade.

Backups e cópias de segurança de informações da OMID Solutions devem ser tratados com o mesmo nível de proteção das informações originais. Fornecedores devem implementar procedimentos seguros para a criação, armazenamento, transporte e restauração de backups, incluindo testes regulares de recuperação.

5.4 Monitoramento e Relatórios

Fornecedores devem implementar sistemas de monitoramento que permitam detectar e responder rapidamente a incidentes de segurança envolvendo informações da OMID Solutions. Estes sistemas devem gerar logs detalhados de todas as atividades relacionadas ao acesso e processamento de nossas informações.

Relatórios regulares sobre o status da segurança da informação devem ser fornecidos à OMID Solutions conforme acordado contratualmente. Estes relatórios devem incluir informações sobre incidentes, mudanças nos controles de

segurança, resultados de testes e avaliações, e quaisquer outros aspectos relevantes para a segurança.

Fornecedores devem participar ativamente de auditorias e avaliações de segurança conduzidas pela OMID Solutions ou por terceiros por ela designados. Isso inclui fornecer acesso a documentação, sistemas e pessoal conforme necessário para a condução efetiva destas avaliações.

6. Classificação e Tratamento de Informações

A OMID Solutions utiliza um sistema estruturado de classificação de informações que permite determinar o nível apropriado de proteção para cada tipo de dado. Fornecedores devem compreender e aplicar corretamente esta classificação em todas as suas interações com nossas informações.

6.1 Níveis de Classificação

Informações Públicas

Informações públicas são aquelas que podem ser divulgadas sem restrições e que foram especificamente aprovadas para divulgação pública pela OMID Solutions. Estas informações incluem materiais de marketing aprovados, comunicados de imprensa oficiais, informações disponíveis em nosso website público e outros materiais destinados ao conhecimento geral.

Mesmo sendo classificadas como públicas, estas informações devem ser tratadas com respeito e não podem ser alteradas, distorcidas ou utilizadas de forma que possa prejudicar a reputação da OMID Solutions. Fornecedores devem sempre verificar a autenticidade e atualidade de informações públicas antes de utilizá-las.

Informações Internas

Informações internas são aquelas destinadas ao uso dentro da organização OMID Solutions e seus parceiros autorizados. Estas informações não devem ser divulgadas externamente sem autorização específica, mas podem ser compartilhadas entre colaboradores e fornecedores que tenham necessidade legítima de conhecimento.

Exemplos de informações internas incluem políticas e procedimentos operacionais, estruturas organizacionais, informações de contato de colaboradores, e outros dados que, embora não sejam altamente sensíveis, requerem proteção contra divulgação não autorizada. Fornecedores devem implementar controles básicos de acesso e confidencialidade para estas informações.

Informações Restritas

Informações restritas possuem sensibilidade elevada e seu acesso deve ser limitado apenas a indivíduos específicos que tenham autorização expressa e necessidade comprovada de conhecimento. A divulgação não autorizada destas informações pode causar danos significativos à OMID Solutions, seus clientes ou parceiros.

Esta categoria inclui informações técnicas detalhadas sobre sistemas e infraestrutura, dados financeiros sensíveis, informações sobre clientes específicos, detalhes de contratos comerciais, e propriedade intelectual. Fornecedores que lidam com informações restritas devem implementar controles de segurança reforçados e procedimentos especiais de manuseio.

Informações Confidenciais

Informações confidenciais representam o mais alto nível de sensibilidade e requerem proteção máxima. O acesso a estas informações é extremamente limitado e requer autorização específica da alta direção da OMID Solutions. A divulgação não autorizada pode resultar em danos graves e irreparáveis.

Exemplos incluem estratégias de negócio de longo prazo, informações sobre fusões e aquisições, dados de clientes altamente sensíveis, segredos comerciais, e informações que possam afetar significativamente a posição competitiva da empresa. Fornecedores raramente terão acesso a informações desta categoria, e quando isso ocorrer, controles especiais e acordos específicos serão necessários.

6.2 Procedimentos de Manuseio por Classificação

Para cada nível de classificação, fornecedores devem implementar procedimentos específicos de manuseio que assegurem proteção adequada. Estes procedimentos devem abordar todos os aspectos do ciclo de vida da informação, desde o acesso inicial até o descarte final.

O manuseio de informações públicas, embora menos restritivo, ainda requer cuidados básicos para evitar alterações não autorizadas e garantir que a informação seja utilizada de forma apropriada. Fornecedores devem manter registros de utilização quando solicitado e respeitar quaisquer direitos de propriedade intelectual aplicáveis.

Informações internas requerem controles de acesso baseados em funções, onde apenas colaboradores do fornecedor que necessitem da informação para desempenhar suas funções tenham acesso. Procedimentos de backup e recuperação devem ser implementados, e a informação deve ser protegida contra acesso não autorizado através de medidas técnicas e físicas apropriadas.

Para informações restritas e confidenciais, fornecedores devem implementar controles de segurança de nível empresarial, incluindo criptografia forte, autenticação multifator, monitoramento de acesso, e procedimentos rigorosos de auditoria. O acesso deve ser registrado e monitorado continuamente, com relatórios regulares fornecidos à OMID Solutions.

7. Controles de Segurança Requeridos

Fornecedores devem implementar um conjunto abrangente de controles de segurança que abordem aspectos técnicos, físicos e administrativos da proteção da informação. Estes controles devem ser proporcionais ao nível de risco e à sensibilidade das informações envolvidas.

7.1 Controles Técnicos

Proteção de Sistemas e Redes

Fornecedores devem manter sistemas operacionais e aplicações atualizados com as correções de segurança mais recentes. Um programa formal de gerenciamento de patches deve ser implementado, com procedimentos para avaliação, teste e implementação de atualizações de segurança em tempo hábil.

Firewalls e sistemas de detecção de intrusão devem ser implementados para proteger redes e sistemas que processam informações da OMID Solutions. Estas proteções devem ser configuradas de acordo com o princípio do menor privilégio, permitindo apenas o tráfego estritamente necessário para as operações autorizadas.

Soluções antimalware devem ser implementadas em todos os sistemas que possam ter contato com informações da OMID Solutions. Estas soluções devem ser mantidas atualizadas com as definições mais recentes e configuradas para realizar verificações regulares e em tempo real.

Criptografia e Proteção de Dados

Informações sensíveis da OMID Solutions devem ser protegidas através de criptografia adequada tanto em trânsito quanto em repouso. Os algoritmos de criptografia utilizados devem estar em conformidade com padrões reconhecidos internacionalmente e ser aprovados pela OMID Solutions.

Chaves criptográficas devem ser gerenciadas de acordo com melhores práticas da indústria, incluindo geração segura, distribuição controlada, armazenamento protegido e rotação regular. Fornecedores devem implementar procedimentos para revogação e recuperação de chaves quando necessário.

Certificados digitais utilizados para autenticação e criptografia devem ser obtidos de autoridades certificadoras reconhecidas e mantidos adequadamente durante todo o seu ciclo de vida. Procedimentos devem estar em vigor para renovação oportuna e revogação quando necessário.

7.2 Controles Administrativos

Políticas e Procedimentos

Fornecedores devem manter documentação atualizada de todas as políticas e procedimentos de segurança da informação relevantes para os serviços prestados à OMID Solutions. Esta documentação deve ser revisada regularmente e atualizada conforme necessário para refletir mudanças nos requisitos ou no ambiente operacional.

Procedimentos de resposta a incidentes devem ser estabelecidos e testados regularmente. Estes procedimentos devem incluir critérios claros para classificação de incidentes, escalação apropriada, comunicação com a OMID Solutions, e ações de contenção e recuperação.

Programas de treinamento e conscientização em segurança da informação devem ser implementados para todos os colaboradores que tenham acesso a informações da OMID Solutions. O treinamento deve ser adaptado às funções específicas de cada colaborador e atualizado regularmente para abordar novas ameaças e requisitos.

Gestão de Mudanças

Todas as mudanças em sistemas, processos ou controles que possam afetar a segurança de informações da OMID Solutions devem ser gerenciadas através de um processo formal de controle de mudanças. Este processo deve incluir avaliação de impacto na segurança, aprovação apropriada, teste adequado e documentação completa.

Mudanças emergenciais devem ser tratadas através de procedimentos especiais que permitam implementação rápida quando necessário, mas que ainda mantenham controles adequados de segurança e documentação. Todas as mudanças emergenciais devem ser revisadas e formalizadas posteriormente.

Fornecedores devem notificar a OMID Solutions sobre mudanças significativas que possam afetar a segurança ou a prestação de serviços. Esta notificação deve ocorrer com antecedência adequada para permitir avaliação e planejamento apropriados.

8. Gestão de Acessos

A gestão adequada de acessos é fundamental para garantir que apenas indivíduos autorizados possam acessar informações da OMID Solutions e que este acesso seja limitado ao mínimo necessário para o desempenho de suas funções. Fornecedores devem implementar controles rigorosos de gestão de identidade e acesso.

8.1 Controle de Acesso Lógico

Todos os acessos a sistemas e informações da OMID Solutions devem ser baseados no princípio do menor privilégio, onde usuários recebem apenas os acessos mínimos necessários para desempenhar suas funções específicas. Fornecedores devem implementar sistemas de gestão de identidade que permitam controle granular de permissões.

Autenticação forte deve ser implementada para todos os acessos a informações sensíveis da OMID Solutions. Isso inclui o uso de senhas complexas, autenticação multifator quando apropriado, e outros mecanismos de autenticação aprovados. Senhas devem seguir políticas rigorosas de complexidade e ser alteradas regularmente.

Contas de usuário devem ser únicas e individuais, não sendo permitido o compartilhamento de credenciais entre colaboradores. Contas genéricas ou compartilhadas só podem ser utilizadas em circunstâncias excepcionais e com aprovação específica da OMID Solutions, sempre com controles compensatórios adequados.

8.2 Revisão e Monitoramento de Acessos

Fornecedores devem implementar procedimentos regulares de revisão de acessos para garantir que as permissões concedidas permaneçam apropriadas e necessárias. Estas revisões devem ser conduzidas pelo menos trimestralmente ou conforme especificado em acordos contratuais específicos.

Todas as atividades de acesso a informações da OMID Solutions devem ser registradas em logs detalhados que incluam identificação do usuário, horário de acesso, recursos acessados e ações realizadas. Estes logs devem ser protegidos contra alteração e mantidos pelo período especificado nos acordos contratuais.

Sistemas de monitoramento automatizado devem ser implementados para detectar atividades suspeitas ou não autorizadas. Alertas devem ser configurados para notificar imediatamente sobre tentativas de acesso não autorizado, múltiplas falhas de autenticação, acessos fora do horário normal, ou outras atividades anômalas.

8.3 Provisionamento e Desprovisionamento

Procedimentos formais devem ser estabelecidos para a concessão de novos acessos, incluindo aprovação apropriada, verificação de necessidade de negócio, e documentação adequada. Todos os acessos devem ser aprovados por gestores autorizados antes da implementação.

Quando colaboradores do fornecedor deixarem a organização ou mudarem de função, todos os acessos relacionados a informações da OMID Solutions devem ser imediatamente revogados ou ajustados conforme apropriado. Procedimentos de desligamento devem garantir que esta revogação ocorra de forma oportuna e completa.

Acessos temporários ou de emergência devem ser tratados através de procedimentos especiais que permitam concessão rápida quando necessário, mas com controles adequados e revisão posterior. Todos os acessos temporários devem ter data de expiração definida e ser automaticamente revogados quando não mais necessários.

9. Segurança Física e Ambiental

A proteção física das informações da OMID Solutions é tão importante quanto a proteção lógica. Fornecedores devem implementar controles físicos adequados para proteger equipamentos, mídias de armazenamento e documentos que contenham nossas informações.

9.1 Controles de Acesso Físico

Áreas onde informações da OMID Solutions são processadas ou armazenadas devem ser protegidas através de controles de acesso físico apropriados. Isso inclui o uso de cartões de acesso, biometria, ou outros mecanismos de autenticação física, dependendo da sensibilidade das informações envolvidas.

Visitantes e prestadores de serviços temporários devem ser sempre acompanhados quando em áreas onde informações da OMID Solutions possam estar presentes. Registros de acesso de visitantes devem ser mantidos e incluir identificação, propósito da visita, horário de entrada e saída, e pessoa responsável pelo acompanhamento.

Áreas críticas, como centros de dados, salas de servidores e locais de armazenamento de backup, devem possuir controles de acesso reforçados, incluindo múltiplos fatores de autenticação, monitoramento por vídeo, e sistemas de detecção de intrusão física quando apropriado.

9.2 Proteção Ambiental

Equipamentos que processam ou armazenam informações da OMID Solutions devem ser protegidos contra ameaças ambientais, incluindo fogo, água, variações extremas de temperatura e umidade, e interferência eletromagnética. Sistemas de supressão de incêndio, controle climático e proteção elétrica devem ser implementados conforme apropriado.

Fornecedores devem implementar procedimentos para proteção de equipamentos durante transporte, incluindo embalagem adequada, seguro apropriado, e rastreamento quando necessário. Equipamentos contendo informações sensíveis devem ser limpos ou destruídos de forma segura antes do descarte ou devolução.

Mídias de armazenamento removíveis que contenham informações da OMID Solutions devem ser armazenadas em locais seguros quando não em uso, protegidas contra acesso não autorizado, danos físicos e deterioração. Inventários de mídias devem ser mantidos e verificados regularmente.

10. Gestão de Incidentes de Segurança

Fornecedores devem estabelecer e manter procedimentos efetivos para detecção, resposta e recuperação de incidentes de segurança que possam afetar informações da OMID Solutions. A resposta rápida e adequada a incidentes é crucial para minimizar danos e restaurar operações normais.

10.1 Detecção e Classificação

Sistemas de monitoramento devem ser implementados para detectar automaticamente possíveis incidentes de segurança. Estes sistemas devem ser configurados para identificar atividades suspeitas, tentativas de acesso não autorizado, malware, e outras ameaças potenciais.

Todos os colaboradores do fornecedor devem ser treinados para reconhecer e reportar possíveis incidentes de segurança. Canais claros de comunicação devem ser estabelecidos para permitir reporte rápido e efetivo de incidentes suspeitos.

Incidentes devem ser classificados de acordo com sua severidade e impacto potencial nas operações da OMID Solutions. Critérios claros devem ser estabelecidos para esta classificação, permitindo resposta apropriada e escalação quando necessário.

10.2 Resposta e Contenção

Procedimentos de resposta a incidentes devem incluir ações imediatas de contenção para prevenir a propagação de danos e proteger evidências para investigação posterior. Estas ações devem ser implementadas rapidamente, mas de forma cuidadosa para não destruir evidências importantes.

A OMID Solutions deve ser notificada imediatamente sobre qualquer incidente que possa afetar suas informações ou operações. Esta notificação deve incluir informações preliminares sobre a natureza do incidente, sistemas afetados, e ações de contenção já implementadas.

Equipes de resposta a incidentes devem ser estabelecidas com papéis e responsabilidades claramente definidos. Estas equipes devem incluir representantes técnicos, de segurança, jurídicos e de comunicação conforme apropriado para o tipo de incidente.

10.3 Investigação e Recuperação

Investigações detalhadas devem ser conduzidas para determinar a causa raiz de incidentes, a extensão dos danos, e as ações necessárias para prevenir recorrência. Evidências devem ser coletadas e preservadas de acordo com procedimentos forenses apropriados.

Planos de recuperação devem ser implementados para restaurar operações normais o mais rapidamente possível, mantendo a integridade e segurança das informações. Testes de recuperação devem ser realizados para verificar a efetividade dos procedimentos.

Relatórios pós-incidente devem ser preparados documentando todos os aspectos do incidente, incluindo cronologia, impacto, ações tomadas, e lições aprendidas. Estes relatórios devem ser compartilhados com a OMID Solutions e utilizados para melhorar procedimentos futuros.

11. Conformidade e Auditoria

A OMID Solutions reserva-se o direito de verificar o cumprimento desta política através de auditorias, avaliações e outros mecanismos de monitoramento. Fornecedores devem cooperar plenamente com estas atividades e implementar ações corretivas quando necessário.

11.1 Auditorias e Avaliações

Auditorias de segurança podem ser conduzidas pela OMID Solutions ou por terceiros por ela designados, com frequência determinada pelo nível de risco e

criticidade dos serviços prestados. Fornecedores devem fornecer acesso adequado a sistemas, documentação e pessoal conforme necessário.

Avaliações de vulnerabilidade e testes de penetração podem ser realizados para verificar a efetividade dos controles de segurança implementados. Fornecedores devem cooperar com estas atividades e implementar correções para vulnerabilidades identificadas dentro dos prazos acordados.

Certificações de segurança reconhecidas pela indústria, como ISO 27001, PCI DSS, ou outros relevantes para os serviços prestados, são encorajadas e podem ser requeridas para fornecedores que lidam com informações altamente sensíveis.

11.2 Monitoramento Contínuo

Indicadores de desempenho de segurança devem ser estabelecidos e monitorados regularmente para verificar a efetividade dos controles implementados. Estes indicadores devem ser reportados à OMID Solutions conforme acordado contratualmente.

Fornecedores devem implementar processos de melhoria contínua que utilizem resultados de auditorias, avaliações e monitoramento para aprimorar constantemente seus controles de segurança. Planos de ação devem ser desenvolvidos e implementados para abordar deficiências identificadas.

Mudanças significativas nos controles de segurança, infraestrutura ou processos devem ser comunicadas à OMID Solutions com antecedência adequada para permitir avaliação de impacto e ajustes necessários nos acordos contratuais.

12. Vigência e Atualizações

Esta política entra em vigor imediatamente para todos os novos fornecedores e deve ser implementada por fornecedores existentes dentro do prazo especificado em seus acordos contratuais. A OMID Solutions reserva-se o direito de atualizar esta política conforme necessário para refletir mudanças nos requisitos de negócio, ameaças de segurança ou regulamentações aplicáveis.

12.1 Implementação e Conformidade

Fornecedores têm a responsabilidade de garantir que todos os requisitos desta política sejam adequadamente implementados e mantidos durante toda a duração do relacionamento comercial com a OMID Solutions. Evidências de conformidade devem ser fornecidas quando solicitadas.

O não cumprimento dos requisitos desta política pode resultar em ações corretivas, incluindo suspensão de serviços, rescisão contratual, ou outras medidas

conforme especificadas nos acordos contratuais específicos. A OMID Solutions trabalhará com fornecedores para resolver questões de conformidade sempre que possível.

12.2 Atualizações e Comunicação

Atualizações desta política serão comunicadas a todos os fornecedores através dos canais oficiais de comunicação estabelecidos. Fornecedores são responsáveis por implementar mudanças dentro dos prazos especificados nas comunicações de atualização.

Dúvidas sobre a interpretação ou implementação desta política devem ser direcionadas ao departamento de segurança da informação da OMID Solutions através dos canais de comunicação estabelecidos nos acordos contratuais.

Documento aprovado por:
Diretoria de Operações - OMID Solutions

Data de aprovação: 27/05/2025
Próxima revisão: 27/05/2026

Para questões relacionadas a esta política, entre em contato:
David Hayden Arruda Cruz
Gerente de Inovação e Cibersegurança
E-mail: david.arruda@omidsolutions.com.br