Requisitos Mínimos de Controle do JPMorgan Chase & Co

INTRODUÇÃO

Estes Requisitos Mínimos de Controle ("**Requisitos Mínimos de Controle**") são declarados de maneira geral e o JPMC reconhece que pode haver diversas abordagens para atender a um determinado Requisito Mínimo de Controle. Estes Requisitos Mínimos de Controle não se destinam a substituir as políticas e procedimentos padrão do Fornecedor, mas visam abordar os controles mínimos que o Fornecedor precisa ter como parte de suas políticas e procedimentos. O Fornecedor deve assegurar que continuará adotando os **Requisitos Mínimos de Controle** conforme as tendências de tecnologia mudarem e qualquer nova tecnologia passar a ser utilizada. O Fornecedor precisa documentar com razoável detalhamento como um determinado controle atende a um Requisito Mínimo de Controle. Todos os Requisitos Mínimos de Controle se aplicam aos subcontratados do Fornecedor que processam ou de outra forma têm acesso às Informações Confidenciais do JPMC ou aos Sistemas do JPMC. O termo "deve" nestes Requisitos Mínimos de Controle significa que o Fornecedor envidará esforços comercialmente razoáveis para atender a um Requisito Mínimo de Controle. Quaisquer políticas, procedimentos ou processos necessários mencionados nestes Requisitos Mínimos de Controle precisam ser documentados, revisados e aprovados, com supervisão da gerência, periodicamente. Nem todos os Requisitos Mínimos de Controle se aplicarão a todos os Serviços ou Produtos, mas o Fornecedor precisa ser capaz de mostrar com razoável detalhamento como o Requisito Mínimo de Controle não se aplica. Estes Requisitos Mínimos de Controle não limitam as obrigações do Fornecedor nos termos do Contrato ou da Lei aplicável e não limitam o escopo de uma auditoria pelo JPMC. O Fornecedor precisa estar em conformidade e ter processos para pesquisar, avaliar e estar em conformidade com todas as Leis na(s) jurisdição(ões) aplicável(is).

Conforme usado nestes Requisitos Mínimos de Controle, quaisquer termos em letras maiúsculas não definidos neste documento terão o mesmo significado que o estabelecido no contrato referente ao fornecimento de bens, materiais licenciados e/ou serviços ("Contrato"), aos quais estes Requisitos Mínimos de Controle se relacionem.

GOVERNANÇA DE TECNOLOGIA, RISCO E CONFORMIDADE

- A eficácia dos controles precisa ser regularmente validada por meio de um programa de avaliação de risco documentado e o Fornecedor deve envidar esforços para, em caso de necessidade, eventual remediação ser gerenciada de forma adequada.
- Uma avaliação de risco precisa ser realizada anualmente para verificar a implementação de controles que protegem as operações de negócios e as Informações Confidenciais do JPMC.
- Um conjunto documentado de políticas e procedimentos de segurança precisa reger o recebimento, transmissão, processamento, armazenamento, controle, distribuição, recuperação, acesso, apresentação e proteção de informações, ativos e serviços associados.
- Um processo de gerenciamento para eventuais exceções baseado em risco precisa existir para estabelecer a priorização e remediação ou a aceitação de risco de controles que não foram adotados ou implementados.
- As políticas e responsabilidades de segurança, incluindo treinamento de conscientização sobre segurança cibernética, precisam ser comunicadas e compartilhadas dentro da organização do Fornecedor.

SEGURANÇA FÍSICA E DO AMBIENTE

- Os processos e procedimentos de segurança física e do ambiente precisam estar estabelecidos para instalações com acesso ou armazenamento de Informações Confidenciais do JPMC.

- A equipe do Fornecedor deverá receber acesso às áreas de instalação com base no princípio do mínimo privilégio.
- O acesso físico às instalações precisa ser restrito, com todos os acessos recertificados regularmente.
- Os controles de monitoramento de detecção (por exemplo, CFTV) precisam estar implementados com um período de retenção definido.
- As instalações precisam manter controles de ambiente adequados, inclusive detecção e supressão de incêndio, controle e monitoramento do clima, soluções de energia e energia de reserva e detecção de danos por água.
- Os componentes do controle de ambiente precisam ser monitorados e testados periodicamente.

PROTEÇÃO DE DADOS

- Fornecedores e seus subcontratados devem ter classificação de informações suficiente para fins de proteção de dados.
- As Informações Confidenciais do JPMC precisam ser protegidas e criptografadas com tecnologia de ponta a ponta, abrangendo informação em trânsito e em repouso (inclusive em cópia de segurança "*back-up*"), assim como quando compartilhadas com subcontratados do Fornecedor.
- Todas as credenciais de autenticação (por exemplo, senhas, números de identificação pessoal, autenticação desafio-resposta) precisam ser criptografadas com tecnologia de ponta a ponta, tanto quando em trânsito quanto quando em repouso.
- A política de proteção de dados do Fornecedor precisa abranger criptografia, gerenciamento de ciclo de vida de chave e certificado, algoritmos criptográficos permitidos e comprimentos de chave associados, autenticação de mensagens, funções *hash*, assinaturas digitais e geração de número aleatório.
- A política de proteção de dados deve ser revisada regularmente em relação aos padrões do setor.
- O Fornecedor deve implementar configuração técnica apropriada para a proteção de mídia portátil criptografada.
- Os procedimentos relacionados ao gerenciamento de *cookies* devem estar em conformidade com as Leis

GERENCIAMENTO DE IDENTIDADE E ACESSO

- As políticas e procedimentos de acesso lógico a serem documentados precisam oferecer suporte ao acesso baseado em funções e condicionados ao conceito de "*need to know*" (necessidade do conhecimento), com base no princípio de privilégio mínimo e assegurar a segregação de funções durante o processo de aprovação e provisionamento.
- As políticas de acesso lógico precisam abranger o acesso remoto, a aprovação da solicitação de acesso antes da permissão de acesso e a recertificação periódica de permissão de acesso.
- Cada conta precisa ser identificável de forma individual.
- O processo de gerenciamento de acesso privilegiado e sua política de controle devem ser documentados, abrangendo (i) a separação de contas privilegiadas (no caso de sistema ou de usuários com acesso elevado, que exijam permissões específicas) e de não privilegiadas (pessoais); (ii) uso de ferramentas de verificação de contas privilegiadas ("privileged account discovery"); (iii) a proteção de contas privilegiadas; (iv) os requisitos de revisão de uso pós-atividade; (v) e a garantia de que contas privilegiadas não-interativas (por exemplo, contas do sistema) não estão sendo utilizadas interativamente por usuários finais.
- Uma política de autenticação e autorização, devidamente documentada, precisa abranger todos os sistemas e redes aplicáveis e incluir requisitos de concessão de senha, requisitos de complexidade de senha, redefinições de senha, limites para tentativas de bloqueio, limites para inatividade e garantia de que não será utilizada de forma compartilhada.
- Os direitos de acesso de todos os profissionais e usuários externos às informações e aos recursos de processamento de informações precisam ser removidos após o término de seu vínculo empregatício,

contrato, ou acordo, ou ajustados mediante alteração de função.

- A autenticação multifatorial precisa ser implementada para:
    - O início de qualquer sessão de acesso interativo privilegiado.
    - Conectividade externa à rede do JPMC
    - Aplicações diretamente acessíveis a partir da internet
    - A administração do acesso ao aplicativo.

CONFIGURAÇÃO DE SEGURANÇA

- O Fornecedor precisa implementar controles em sua rede de comunicação para proteger os dados.
- Um diagrama de rede, para incluir todos os dispositivos, assim como um diagrama de fluxo de dados precisa ser mantido de forma atualizada.
- Os dispositivos de rede precisam ter relógios internos sincronizados com fontes de tempo confiáveis.
- As configurações de segurança padrão, usando os princípios de mínimos funcionalidade/privilégios, precisam ser estabelecidas e a proteção da segurança demonstrada.
- Os sistemas de informação precisam ser implantados com configurações de segurança adequadas e revisados periodicamente para manter conformidade com as políticas e padrões de segurança do Fornecedor.
- Desvios de linhas básicas ("*baselines*") de configuração de segurança precisam ser identificados, relatados e corrigidos.
- Precisam existir mecanismos de proteção contra códigos maliciosos ("*malware*") para detectar e/ou prevenir contra *malware* e outras ameaças.
- Os mecanismos de proteção contra *malware* precisam ser configurados para realizar varreduras em tempo real ou programadas de forma a alertar quando um *malware* for descoberto.
- Todos os dispositivos e mecanismos de proteção contra *malware* precisam ser mantidos atualizados com as definições e os s*oftwares* de antivírus mais recentes.
- Os sistemas de detecção e prevenção de intrusão baseados em rede e host precisam ser implantados com os eventos gerados e alimentados em sistemas centralizados para análise.
- O Fornecedor precisa ter políticas, procedimentos e controles que garantam o controle adequado de um sistema de correio eletrônico e/ou de mensagens instantâneas que exibam e/ou contenham informações do JPMC.
- Os controles preventivos precisam bloquear mensagens e anexos maliciosos, assim como impedir o encaminhamento automático de e-mails.

OPERAÇÕES DE SEGURANÇA

- A equipe do Fornecedor precisa ser treinada para identificar e relatar suspeitas de falhas de segurança, atividades suspeitas, e eventos/incidentes de segurança.
- A tecnologia, processos e/ou soluções de Prevenção de Perda de Dados (*Data Loss Prevention* - "**DLP**") precisam ser implantados para proteger contra o vazamento de Informações do JPMC.
- O Fornecedor precisa ter uma política e um procedimento de resposta a eventos/incidentes de segurança.
- A programação de retenção para diversos logs precisa ser definida e seguida.
- Logs de eventos de segurança de sistemas de informação precisam ser coletados, gerenciados centralmente, analisados e correlacionados com o objetivo de detectar comportamentos anômalos que possam indicar eventos/incidentes maliciosos.
- É preciso estabelecer um programa de detecção, prevenção e mitigação de fraudes e ameaças, processos e procedimentos para monitorar e relatar ocorrências reais e suspeitas de fraude e notificação e comunicação específicas, internamente e para o JPMC.
- O Fornecedor deve ter um procedimento para realizar análises forenses digitais, inclusive coleta de dados, preservação de dados/evidências para análises futuras, análises, relatórios de descobertas e

devidas conclusões.

- Um processo deve estar em operação para realizar simulações de ataque em um ambiente segregado, inclusive exercícios de engenharia social (por exemplo, *phishing*), testes "*red teaming*" e testes de simulação de cenário de desastre ("*tabletop exercises*") com relatórios adequados, correção/aceitação e rastreamento de descobertas.
- Acesso a soluções de e-mail não corporativo/pessoal e mensagens instantâneas deve ser restrito.

GERENCIAMENTO DE VULNERABILIDADE

- O Fornecedor precisa reunir continuamente dados de inteligência de vulnerabilidade, tendo em vista ameaças existentes e emergentes, assim como de ataques reais que podem impactar seus sistemas.
- Varreduras de vulnerabilidade (autenticadas e não autenticadas) e testes de penetração precisam ser realizados em redes e aplicativos internos e externos periodicamente e antes do provisionamento do sistema para todos os sistemas que processam, armazenam ou transmitem Informações Confidenciais do JPMC.
- Quaisquer vulnerabilidades críticas identificadas durante varreduras de vulnerabilidade ou teste de penetração precisam ser priorizadas e corrigidas dentro de um período de tempo bem definido, proporcional ao risco de vulnerabilidade.

PRIVACIDADE

- O Fornecedor precisa implementar controles eficazes para assegurar o processamento adequado e a proteção de dados pessoais.
- Números de documentos de identidade ou outros identificadores nacionais não devem ser utilizados como IDs de usuário para *log-on* em aplicativos.
- A avaliação do impacto da privacidade precisa ser realizada durante a fase de concepção do desenvolvimento do sistema para avaliar o impacto nos dados pessoais e revisar o escopo do monitoramento.
- A avaliação do impacto da privacidade não estará em conflito com nenhuma Lei aplicável.
- O Fornecedor precisa ter procedimentos para obter o consentimento dos usuários para coletar dados pessoais, dando aos usuários a capacidade de acessar, corrigir, cancelar, excluir, restringir, tornar portátil ou se opor a seu processamento.
- Um aviso de privacidade ou banner de informações precisa estar disponível, requerendo reconhecimento pelo usuário final sempre que os dados pessoais forem coletados, transmitidos, processados ou armazenados.
- Os procedimentos de coleta de dados pessoais exigidos pela Lei precisam ser previamente definidos e as restrições à sua divulgação precisam ser documentadas.
- O Fornecedor deve possuir um processo para notificar o JPMC sobre qualquer evento que possa afetar ou afete a confidencialidade, integridade ou disponibilidade de dados pessoais, incluindo intrusão não autorizada ou suspeita em sistemas que armazenam tais dados pessoais.

DESENVOLVIMENTO DE TECNOLOGIA

Ciclo de vida de desenvolvimento do sistema ("***System Development Life Cycle***" ou "SDLC")

- Os Fornecedores precisam operar um processo estabelecido de Ciclo de Vida de desenvolvimento de sistema –"SDLC".
- O procedimento de SDLC precisa ser estabelecido, documentado e aplicado para identificar e corrigir defeitos, vulnerabilidades, erros de codificação e falhas de projeto antes de entrar em produção usando uma abordagem baseada em risco.
- O SDLC precisa estabelecer os requisitos de controle para o desenvolvimento de *software* que são aplicáveis a qualquer *software* e estrutura de desenvolvimento ou modelo usados.

- O SDLC precisa incluir uma revisão de design seguro e controles preventivos e de detecção para identificar vulnerabilidades e falhas de desenho.
- Os requisitos funcionais e não funcionais devem ser continuamente identificados e implementados para evitar que o *software* se torne obsoleto.

Software de terceiros

- O código ou *software* de terceiros e de fonte aberta usados precisa ser devidamente licenciado, inventariado e, quando licenciado comercialmente, ter suporte total do fornecedor.

OPERAÇÕES DE TECNOLOGIA

- Os procedimentos operacionais documentados precisam possuir operação correta e segura dos ativos..
- Os procedimentos operacionais precisam incluir o monitoramento da capacidade e desempenho,
- Alterações no sistema de produção, rede, aplicativos, estruturas de arquivos de dados, outros componentes do sistema e alterações físicas/ambientais precisam ser monitoradas e controladas por meio de um ambiente formal de controle de alterações.
- As alterações devem ser testadas antes da implementação e revisadas quanto ao impacto.
- As alterações precisam ser aprovadas antes da implementação e avaliada depois da implementação para assegurar que os resultados desejados tenham sido alcançados.
- Um procedimento de gerenciamento de alteração de emergência precisa ser documentado.
- Quaisquer alterações que afetem materialmente os serviços do JPMC precisam ser comunicadas ao JPMC antes da implementação.
- Os ativos de infraestrutura devem seguir um processo de manutenção de tecnologia documentado e aprovado.

RELACIONAMENTOS COM TERCEIROS

- Os subcontratados do Fornecedor precisam ser identificados, avaliados, gerenciados e monitorados de acordo com os termos do Contrato com o JPMC, inclusive conformidade com os Requisitos Mínimos de Controle do JPMC aplicáveis a esses serviços.

GERENCIAMENTO DE DOCUMENTOS OU REGISTROS

- Fornecedores e seus subcontratados que fornecem dados regularmente ao JPMC devem manter e fornecer um dicionário de dados ou artefato de classificação de dados equivalente, incluindo quaisquer metadados acordados para dados fornecidos ao JPMC.
- Fornecedor e seus subcontratados devem ter controles para permitir que o JPMC valide que um conjunto completo de dados foi recebido em um formato acordado. O Fornecedor deve ter um processo para notificar o JPMC sobre erros de dados transmitidos para ou do JPMC de acordo com as especificações de qualidade para precisão, pontualidade e integridade dos dados.
- Todos os dados JPMC fornecidos e armazenados pelo Fornecedor e subcontratados dependentes devem ser armazenados e retidos de maneira que:
    - inclui a capacidade de acessar e recuperar os dados conforme necessário;
    - evita perdas devido à deterioração da mídia ou obsolescência da tecnologia;
    - fornece salvaguardas razoáveis contra perigos comuns, perigos provocados pelo homem e desastres;
    - está em conformidade com as Leis e obrigações contratuais aplicáveis;
    - protege os dados de acesso/alteração não autorizado.
- No caso de o Fornecedor estar mantendo documentos ou registros em nome do JPMC, o Fornecedor precisa manter e validar com o JPMC (no mínimo anualmente) um inventário completo e exato de

todos os tipos com os seguintes atributos para cada um:

- Propriedade
- Tipo de documento/registro
- Classificação
- Requisitos de retenção/destruição (e execução desses requisitos)
- Localização

- Os Fornecedores e subcontratados que recebam, enviam, transmitam, armazenem, criem, gerem, coletem, controlem, processem ou tenham acesso às Informações Confidenciais do JPMC, o farão exclusivamente para prestar Serviços ao JPMC.
- Os Fornecedores e subcontratados precisam estar habilitados a manter a origem dos dados.

GERENCIAMENTO DE ATIVOS DE TECNOLOGIA

- O Fornecedor precisa ter uma política e procedimento de registro de ativos de tecnologia suficiente, inclusive identificadores exclusivos para todos os ativos, classificação adequada, propriedade do ativo, localização do ativo e licenciamento adequado, requisitos legais, regulatórios, contratuais ou de suporte.
- O Fornecedor precisa manter uma estrutura de governança de inventário de ativos de tecnologia adequada para incluir alterações registradas nos registros de ativos, cópia de segurança suficiente dos registros de ativos, validação de integridade anual dos registros de ativos, recertificação de propriedade de ativos, atualizações oportunas de registro de ativos quando os registros de ativos são alterados, auditorias de licença regulares de ativos, e remediação de ativos não autorizados.
- Um programa de gerenciamento do ciclo de vida de ativos de tecnologia precisa ser implementado que inclua o status exato do ciclo de vida de todos os ativos, identificação de ativos que não estão em conformidade com a política de gerenciamento do ciclo de vida e notificação aos proprietários de ativos de ativos não compatíveis.
- Um programa de provisionamento e descarte de ativos de tecnologia precisa estar implementado para incluir somente a aquisição de ativos de tecnologia de Fornecedores de origem adequada e o descarte/remoção/exclusão de todos os ativos de tecnologia de maneira segura quando eles chegarem ao fim da vida útil.
- O Fornecedor deve garantir que os ativos sejam transportados de maneira segura.

GERENCIAMENTO DE INCIDENTES E EVENTOS

- Os procedimentos de gerenciamento de incidentes, eventos ou problemas precisam incluir seu rastreamento sistemático, desde a descoberta até a sua resolução.
- A política e os procedimentos de gerenciamento de eventos do Fornecedor precisam levar em conta a detecção, análise e apresentação de eventos anômalos que indicam desvio da norma além de um limite definido e envolver o JPMC por meio do processo de gerenciamento de incidentes.
- A política e os procedimentos de gerenciamento de incidentes precisam incluir as responsabilidades da equipe do Fornecedor e a identificação das partes a serem notificadas em caso de um evento/incidente de segurança da informação.
- A política e os procedimentos de gerenciamento de incidentes do Fornecedor também precisam incluir priorização, funções e responsabilidades, escalonamento interno, notificação ao JPMC, rastreamento e relatórios, contenção e remediação e preservação de dados para manter a integridade forense.
- A política de gerenciamento de problemas do Fornecedor deve incluir a documentação da análise de causa raiz, implementação de correção permanente, ações preventivas e oportunidades de melhoria de serviço, fornecendo conclusões ao JPMC.

RESILIÊNCIA DE NEGÓCIOS

- O Fornecedor precisa ter planos de resiliência de negócios abrangentes e formais para permitir a recuperação oportuna, ordenada e sustentável de negócios, processos de suporte, operações e componentes de tecnologia dentro de um prazo acordado.
- O Fornecedor precisa realizar uma Análise de Impacto nos Negócios (*Business Impact Analysis* - "**BIA**") para determinar a criticidade de seu processo de resiliência de negócios e definir um Objetivo de Tempo de Recuperação (*Recovery Time Objective* - "**RTO**") para todos os processos que utilizar para fornecer suporte aos serviços ou funções que estão sendo executados para o JPMC.
- Os planos de resiliência de negócios precisam identificar os recursos-chave e abordar as interrupções de negócios desses recursos que dão suporte a todos os serviços do JPMC, inclusive aqueles fornecidos por subcontratados do Fornecedor.
- Os planos de resiliência precisam ter recursos de recuperação mínimos para atender aos objetivos de RTO e o nível de serviço do JPMC, visando abordar adequadamente os seguintes cenários de interrupção:
    - Perda de Pessoal
    - Perda de Local
    - Perda de Aplicação (quando aplicação para recuperação de desastres estiver disponível)
    - Perda de fornecedores terceiros (quando a recuperação de fornecedor terceiro estiver disponível)
- Os planos de resiliência precisam ter estratégias/locais de trabalho alternativos aceitáveis para assegurar que os compromissos de nível de serviço sejam atendidos.
- Os planos de recuperação do Fornecedor devem ser atualizados, revisados e aprovados pelo menos uma vez por ano ou quando ocorrerem mudanças materiais no ambiente operacional do fornecedor.
- Os planos de resiliência precisam ser testados regularmente e as deficiências/falhas observadas precisam ser tratadas em tempo hábil, e os testes devem:
    - ser conduzidos em condições comparáveis à produção
    - demonstrar recuperação dentro dos de tempos e recuperação estabelecidos
    - ocorrer anualmente
- Qualquer alteração que possa afetar a recuperação do processo ou infraestrutura pode envolver, mas não está limitada a, alterações na estratégia de negócios, serviço, processo, ativos e obrigações regulatórios/legais, resultando em alterações significativas no BIA ou planos requererão um novo teste dos planos de recuperação afetados pela alteração significativa.

RESILIÊNCIA DE TECNOLOGIA

- O Fornecedor precisa ter planos formais de recuperação de tecnologia para identificar os recursos e especificar as ações necessárias para ajudar a minimizar as perdas em caso de interrupção dos serviços fornecidos ao JPMC ou dos recursos que suportam esses serviços.
- Os planos de recuperação do Fornecedor precisam identificar os próprios processos críticos do Fornecedor, apoiando ativos, dependências, pontos críticos de falha, equipe de recuperação e recursos de recuperação para lidar com interrupções de negócios para processos que suportarem serviços do JPMC.
- O Fornecedor precisa ter planos de recuperação de tecnologia (inclusive aqueles específicos para cenários de ataque cibernético) com a capacidade para limitar a interrupção do serviço.
- A capacidade de recuperação de tecnologia precisa incluir a capacidade de se recuperar de um evento cibernético destrutivo em que:
    - os sistemas primários (produção) foram comprometidos ou destruídos, e
    - os sistemas primário e secundário (DR) foram comprometidos ou destruídos.
- Os planos devem incluir como reimplantar um aplicativo e restaurar os dados associados após uma perda.
- Os planos de recuperação também precisam incluir subcontratados do Fornecedor, inclusive

provedores de serviços em nuvem.

- Os planos de recuperação precisam ser testados regularmente, usando testes suficientes, que incluam o teste de estratégias de longo prazo. As falhas de teste devem ser testadas novamente dentro de um período de tempo razoável.
- Os aplicativos e hosts associados devem empregar uma política de backup para atender a capacidade de recuperação total do aplicativo. A política deve definir conjuntos de dados, frequências, critérios para um backup bem-sucedido, requisitos de teste anual, requisitos de armazenamento externo e períodos de retenção. A política de backup deve ser revisada e recertificada anualmente.
- Os planos de recuperação de tecnologia precisam assegurar a recuperação oportuna, ordenada e sustentável de componentes de tecnologia dentro de um RTO definido no Contrato, em caso de evento de perda, planejada ou não, da implementação da aplicação ou do local de implantação.
- Qualquer evento que possa afetar planos de recuperação, inclusive eventos de alterações significativas na equipe, estrutura organizacional, tecnologia, localização ou estratégia requererá a elaboração de novos planos de recuperação, bem como os respectivos testes, conforme necessário dada a significância do evento.
- O Fornecedor precisa ter uma estrutura de gerenciamento de crise, inclusive notificação inicial ao JPMC e contato contínuo com o JPMC durante um incidente que afete os serviços executados pelo Fornecedor.
- As Informações Confidenciais do JPMC precisam estar disponíveis mediante solicitação, em um formato padrão do setor, de modo a assegurar portabilidade e interoperabilidade.

SEGURANÇA ORGANIZACIONAL

- A equipe do Fornecedor alocada para prestar os Serviços do JPMC precisa revisar o Código de Conduta do Fornecedor do JPMC disponível no site do JPMC.
- A equipe do Fornecedor precisa notificar o JPMC no caso de qualquer conflito de interesse potencial ou real entre as atividades comerciais externas e relações pessoais da equipe do Fornecedor e os negócios, clientes ou funcionários do JPMC.
- O Fornecedor precisa fornecer treinamento à sua equipe sobre as responsabilidades do trabalho, incluindo treinamento de conscientização sobre segurança cibernética, e assegurar que a equipe conclua qualquer treinamento que for designado pelo JPMC.
- O Fornecedor precisa realizar um processo formal de análise de desempenho e avaliação de sua equipe.
- O Fornecedor precisa manter organogramas atualizados que representem as principais responsabilidades de gerenciamento dos Serviços prestados ao JPMC, inclusive quando envolver subcontratados.
- O Fornecedor precisa realizar verificações de antecedentes em sua equipe conforme apropriado.
- O Fornecedor precisa assegurar que sua equipe tenha concordado com as obrigações de não divulgação ou confidencialidade antes de designá-los para prestar os Serviços ao JPMC e fornecer acesso aos sistemas e informações do JPMC.

CONTATO COM CLIENTE

- Se estiver fornecendo atendimento ao cliente (por exemplo, agentes de contato do cliente e operações relacionadas), o Fornecedor precisa ter definido e aplicado procedimentos operacionais que assegurem a confidencialidade, integridade e disponibilidade das Informações Confidenciais do JPMC, assim como a prestação de serviços e o fornecimento de outros produtos em conformidade com o(s) respectivo(s) contrato(s).
- O Fornecedor precisa manter e implementar procedimentos eficazes para a autenticação de cada cliente, inclusive considerando orientações eventualmente fornecidas pelo JPMC.
- Fornecedor que seja agente de contato com o cliente precisa receber treinamento de privacidade (por

exemplo, abordando o manuseio adequado de dados pessoais tendo em vista as Leis e regulações de privacidade), conforme especificado no(s) respectivo(s) contrato(s) ou conforme indicado pelo JPMC.

- Quaisquer reclamações recebidas em relação ao JPMC ou em relação a quaisquer serviços prestados para ou em nome do JPMC precisam ser comunicadas ao JPMC, conforme especificado no(s) respectivo(s) contrato(s) ou conforme indicado pelo JPMC.