Requisitos de segurança para fornecedores da Alludo

Índice

Introdução

Este documento descreve as práticas de segurança da informação, continuidade dos negócios e privacidade das empresas do grupo Alludo (coletivamente "Alludo"), bem como o programa de avaliação das medidas de segurança e continuidade dos fornecedores da Alludo. Os processos, os procedimentos, os requisitos e as obrigações mencionados neste documento são coletivamente denominados "Padrões Alludo".

Este documento **Requisitos de segurança para fornecedores da Alludo** informa os fornecedores que oferecem bens e serviços ("Fornecedores") sobre as expectativas de segurança, continuidade dos negócios e privacidade que a Alludo espera que cumpram ao prestarem serviços. Os fornecedores devem implementar esses requisitos seguindo as melhores práticas do setor e suas políticas de segurança corporativa. A Alludo não será responsável por quaisquer problemas enfrentados pelos fornecedores, incluindo perda de dados ou danos a equipamentos, independentemente da causa.

Em caso de qualquer inconsistência entre este documento e um acordo por escrito, os termos do acordo por escrito prevalecerão. Os fornecedores também devem cumprir quaisquer requisitos regulatórios locais, nacionais ou regionais. Caso surja um conflito entre este documento e os regulamentos aplicáveis, os fornecedores deverão notificar a Alludo e sugerir controles alternativos para manter padrões equivalentes de segurança, continuidade ou privacidade.

Visão geral dos requisitos de segurança para fornecedores

A Alludo tem a responsabilidade de proteger suas informações restritas e confidenciais contra divulgação ou acesso não autorizado. Para isso, a Alludo implementa os Padrões Alludo (padrões internos de segurança da informação, continuidade dos negócios e privacidade) para garantir que essas informações restritas e confidenciais sejam protegidas e que os serviços prestados pela Alludo estejam continuamente disponíveis. Para garantir a conformidade da Alludo com os padrões internos e os requisitos regulatórios relacionados à segurança da informação e à continuidade dos negócios, a Alludo exige que seus fornecedores sigam os Padrões Alludo descritos neste documento.

Por sua vez, caso um fornecedor delegue ou subcontrate qualquer parte de suas obrigações estabelecidas no acordo com a Alludo ou contrate outro fornecedor para prestar serviços direta ou indiretamente à Alludo, o fornecedor deverá exigir que esse fornecedor implemente e administre um plano e um programa de proteção de informações que esteja em conformidade com os Padrões Alludo. A Alludo está comprometida em trabalhar de forma razoável com seus fornecedores para ajudá-los a atender aos requisitos de conformidade relacionados aos Padrões Alludo. A extensão da aplicabilidade desses Padrões Alludo a um fornecedor específico variará dependendo do tipo de serviço e dos produtos oferecidos por esse fornecedor à Alludo.

Controle de acesso e identidade

Obrigações do fornecedor:

1. **Controle de acesso e gerenciamento de usuários**:
    1.1. Uma política de controle de acesso documentada deve estar implementada e ser revisada pelo menos uma vez por ano.
    1.2. As permissões, os direitos de acesso e as funções de usuário devem estar definidos e documentados.
    1.3. Processos padrão para a integração e o desligamento de usuários devem estar implementados, incluindo o registro das aprovações relevantes.
    1.4. O acesso aos componentes da infraestrutura de TI deve ser concedido com base no princípio do menor privilégio e gerenciado por meio de ferramentas de gerenciamento de identidade (por exemplo, Active Directory, OKTA ou similar).
    1.5. O acesso individual a sistemas, recursos de rede e outros recursos de TI deve ser formalmente aprovado e controlado por meio de IDs de usuário exclusivos e senhas individuais.

1.6. A segregação de funções deve ser mantida durante a criação/alteração de IDs de usuário e a atribuição de privilégios.

2. **Políticas de senha e autenticação**:
   2.1. Os usuários devem alterar sua senha no login inicial.
   2.2. As senhas devem atender aos requisitos padrão do setor, incluindo comprimento, expiração, complexidade, histórico de senhas, tentativas malsucedidas, duração do bloqueio da conta, validade da senha e alteração no primeiro logon.
   2.3. Mecanismos seguros devem ser usados para fornecer senhas de usuário e validar identidades de usuário antes do início das redefinições de senhas.
   2.4. Os sistemas que não oferecem suporte à autenticação IdP ou que precisam ser desenvolvidos como soluções independentes devem ser configurados para impor autenticação forte, com uma configuração que seja igual ou mais rigorosa do que a definida nas políticas centrais de senha e controle de acesso.
   2.5. Todos os sistemas e aplicativos devem ser configurados para usar procedimentos de logon seguros por meio de mecanismos aprovados de gerenciamento de identidade e acesso.
   2.6. Os sistemas e os aplicativos devem ser configurados para encerrar sessões ociosas, a fim de evitar acessos não autorizados.

3. **Gerenciamento de acesso privilegiado**:
   3.1. O acesso privilegiado aos recursos deve ser restrito a funções de usuário definidas e deve ser aprovado por pessoal autorizado.
   3.2. As contas de usuário privilegiadas devem ser configuradas para usar autenticação multifator.
   3.3. Os privilégios que não são mais necessários devem ser revogados imediatamente.
   3.4. O uso de credenciais administrativas deve ser restrito a circunstâncias limitadas, como solução de problemas, e os usuários devem realizar as operações diárias usando credenciais com menos privilégios.
   3.5. O acesso à infraestrutura de TI, aos sistemas, aos dispositivos de rede e aos aplicativos essenciais (por exemplo, acesso remoto, servidores críticos, dispositivos de rede) deve ser protegido usando a autenticação multifator.

4. **Revisão e monitoramento de acesso**:
   4.1. Devem ser realizadas revisões periódicas dos direitos de acesso e as exceções identificadas devem ser prontamente resolvidas.
   4.2. Uma reconciliação de todos os IDs de usuário (incluindo domínio, aplicativos, dispositivos de rede, sistemas de TI, middleware, bancos de dados, etc.) deve ser realizada, no máximo, uma vez por ano, com ações corretivas imediatas adotadas para quaisquer discrepâncias identificadas.
5. **Gerenciamento de terceiros e fornecedores**:
   5.1. O acesso de fornecedores terceirizados a redes e sistemas deve ser rigidamente controlado e concedido somente em caso de necessidade e com aprovação formal.
   5.2. As credenciais padrão fornecidas pelo fornecedor devem ser alteradas antes que sistemas, aplicativos, dispositivos de rede ou outros dispositivos da infraestrutura de TI sejam colocados em produção.

6. **Considerações especiais sobre acesso**:
   6.1. IDs genéricos e compartilhados não devem ser usados, a menos que sejam formalmente justificados e aprovados pela alta gerência, com mecanismos para rastrear o uso e associar ações a indivíduos.
   6.2. Todo acesso administrativo não realizado pelo console deve ser criptografado usando algoritmos de criptografia aprovados pelo setor e deve ser proibido o uso de protocolos inseguros (por exemplo, telnet/ftp) para acesso administrativo não realizado pelo console.

Gerenciamento de ativos

Obrigações do fornecedor:

7. **Inventário e gerenciamento de ativos**:
   7.1. Inventários completos de ativos devem ser mantidos, registrando detalhes essenciais como dados de contato, localização e informações do proprietário dos ativos,
   7.2. Os registros de ativos de tecnologia da informação, incluindo hardware, sistemas operacionais, aplicativos e bancos de dados, devem ser regularmente atualizados e revisados para garantir a precisão.
   7.3. Procedimentos de gerenciamento de ativos e controles de configuração devem ser estabelecidos e mantidos para gerenciar a disponibilidade de ativos críticos e as configurações de sistemas de rede e informações vitais.

8. **Classificação e identificação de informações**:
   8.1. Uma política de classificação de informações, acompanhada de procedimentos e diretrizes de apoio, deve ser mantida. Todos os ativos devem ser identificados de acordo com as instruções estabelecidas e as informações devem ser classificadas e protegidas com base nos níveis de classificação definidos.

9. **Manuseio de ativos**:
   9.1. Diretrizes de gerenciamento de ativos para o manuseio adequado devem ser mantidas e comunicadas a todos os funcionários e prestadores de serviços aplicáveis.
   9.2. Procedimentos documentados devem estar em vigor para proteger ativos de informação, identificar ativos que devem ser descartados e garantir o descarte seguro desses ativos.
   9.3. Processos devem ser estabelecidos para garantir que os ativos alocados sejam prontamente devolvidos à equipe de gerenciamento de ativos correspondente após o término ou a rescisão do vínculo empregatício, contrato ou acordo.

10. **Gerenciamento de dispositivos móveis e mídias removíveis**:
    10.1. Políticas e procedimentos para controlar os dispositivos móveis (incluindo BYOD) usados para armazenar, transmitir ou processar informações empresariais devem ser implementados. Medidas de proteção adequadas devem ser exigidas antes de permitir que dispositivos móveis acessem informações e recursos empresariais.
    10.2. O uso de dispositivos removíveis de armazenamento em massa deve ser criptografado para garantir a segurança dos dados.

11. **Conformidade de software**:
    11.1. Deve ser proibido o uso de software não licenciado ou não aprovado. É preciso haver processos para identificar quaisquer violações e tomar as medidas necessárias para solucioná-las.

Operações de TI

Obrigações do fornecedor:

12. **Operações críticas do sistema**:
    12.1. Procedimentos para a operação de redes e sistemas de informações críticos devem ser estabelecidos e mantidos, abrangendo:
        12.1.1. Processos formais de aprovação para acesso a ativos de TI.
        12.1.2. Mecanismos robustos de autenticação para todas as tecnologias (por exemplo, VPN, logon no Windows).
        12.1.3. Revisão regular dos direitos de privilégio.
        12.1.4. Identificação dos locais de rede para tecnologias críticas com base nos requisitos de continuidade dos negócios.
13. **Gerenciamento de mudanças**:
    13.1. Um processo abrangente de gerenciamento de mudanças deve ser implementado para sistemas de TI, aplicativos, bancos de dados e componentes de rede, garantindo:
        13.1.1. O registro, a revisão, o teste e a aprovação formal de todas as mudanças.
        13.1.2. Planos de reversão de modificações que possam causar interrupções.
14. **Outros**:
    14.1. Os sistemas e os componentes de rede que processam informações sigilosas e confidenciais devem estar sujeitos a verificações de monitoramento de integridade de arquivos.
    14.2. Todos os sistemas e componentes de rede devem estar configurados para usar fontes NTP (Network Time Protocol) autorizadas para sincronização precisa do tempo.
    14.3. Processos regulares de manutenção proativa e preventiva devem ser estabelecidos para todos os aplicativos, dispositivos de rede, máquinas de usuários finais e sistemas críticos.
    14.4. Os conjuntos de regras de firewall e roteador devem ser revisados periodicamente ou de acordo com os padrões do setor, sendo prontamente removidas as regras desnecessárias ou não autorizadas.
    14.5. Controles devem ser implementados para manter a integridade das informações e do software em todo o ambiente de TI.

Segurança de recursos humanos

Obrigações do fornecedor:

15. **Verificações de antecedentes**:

15.1. Políticas e procedimentos devem ser estabelecidos e mantidos para a realização de verificações de antecedentes.

15.2. Verificações adequadas de antecedentes de funcionários e prestadores de serviços devem ser realizadas antes da integração, na medida permitida por lei, com base em suas funções e responsabilidades.

16. **Gerenciamento de mudanças no quadro de pessoal**:

16.1. Um processo deve ser implementado para gerenciar mudanças no quadro de pessoal ou em suas funções e responsabilidades, incluindo a orientação dos novos colaboradores sobre as políticas e os procedimentos relevantes.

16.2. Após mudanças no quadro de pessoal, os direitos de acesso, os crachás, o equipamento e outros recursos deverão ser revogados imediatamente quando não forem mais necessários ou permitidos.

17. **Aplicação de políticas**:

17.1. Um processo disciplinar claro deve ser implementado e mantido para funcionários que violarem as políticas de segurança.

17.2. A responsabilização por violações das políticas de segurança deve ser assegurada por meio de medidas contratuais apropriadas. Isso inclui a incorporação de cláusulas relevantes em contratos de trabalho para funcionários e acordos de serviço para terceirizados.

Treinamento sobre segurança e privacidade

Obrigações do fornecedor:

18. O treinamento sobre segurança e privacidade deve ser obrigatório para todos os funcionários e prestadores de serviços. Esse treinamento deve ser concluído no momento da contratação inicial e anualmente ou em intervalos menores depois disso.
19. Os funcionários e os prestadores de serviços com responsabilidades significativas em segurança de TI devem passar por treinamento anual especializado, adaptado às suas obrigações e funções de segurança específicas.
20. A gerência deve ter acesso a ferramentas e sistemas que permitam monitorar e acompanhar o progresso do treinamento de seus funcionários e prestadores de serviços.
21. O programa de treinamento e conscientização da organização deve passar por revisões e atualizações periódicas. Esse processo deve considerar a evolução dos requisitos de negócios, as mudanças na legislação e as lições aprendidas com incidentes de segurança anteriores.

Governança e segurança da informação

Obrigações do fornecedor:

22. **Governança e estrutura de segurança**:

22.1. O fornecedor deve implementar uma estrutura reconhecida de padrões de segurança (por exemplo, NIST CSF, RMF, 800-53, ISO 27001, CIS) para governança de cibersegurança e informações. Essa estrutura deve incluir:

22.1.1. Políticas e procedimentos abrangentes de cibersegurança e informações, sujeitos a revisão anual, aprovação formal e comunicação em toda a organização.

22.1.2. Uma estratégia bem definida de segurança da informação, alinhada aos objetivos de negócios.
22.1.3. Processos robustos de governança e gerenciamento de riscos, abordando especificamente os riscos de cibersegurança e informações.
22.1.4. Mecanismos de conformidade para atender aos requisitos legais e regulatórios relacionados às informações e à cibersegurança.

22.2. Caso não siga uma estrutura de segurança reconhecida, o fornecedor deverá apresentar um relatório demonstrando que seu ambiente passou por uma auditoria.
22.2.1. Um plano de correção para os problemas identificados, incluindo prazos esperados, deverá ser acordado mutuamente entre o fornecedor e a Alludo.

23. Liderança e estrutura organizacional:

23.1. Funções e responsabilidades adequadas para segurança da informação e cibersegurança devem ser definidas e implementadas em toda a organização.

24. Gerenciamento e avaliação de riscos:

24.1. Uma estrutura formal de gerenciamento de riscos aprovada pela alta gerência deve estar em vigor para:
24.1.1. Identificar ameaças internas e externas.
24.1.2. Avaliar a confidencialidade das informações/dos dados envolvidos.
24.1.3. Avaliar os possíveis impactos nos negócios.
24.1.4. Avaliar ameaças, vulnerabilidades e riscos correspondentes.
24.1.4.1. Todos os riscos e ameaças identificados devem ser priorizados e medidas devem ser adotadas em tempo hábil para atenuar os riscos de forma apropriada.
24.1.4.2. Processos e/ou ferramentas devem ser implementados para identificar eventos que possam interromper as operações essenciais para os fins comerciais da organização.
24.1.4.3. O fornecedor deverá notificar a Alludo imediatamente se não conseguir corrigir ou reduzir qualquer risco significativo que possa impactar o serviço prestado.

25. Monitoramento de desempenho e conformidade:

25.1. Processos devem estar em vigor para identificar, registrar e acompanhar todos os requisitos legais, regulatórios e contratuais aplicáveis à organização.

25.2. Avaliações periódicas devem ser realizadas para validar a conformidade com obrigações legais, regulatórias e contratuais. Os registros dessas avaliações devem ser mantidos e as lacunas identificadas devem ser atenuadas sem demora indevida.

25.3. As políticas, os procedimentos e as diretrizes devem ser revisados pelo menos uma vez por ano e atualizados de acordo com os requisitos legais, regulatórios e contratuais.

25.4. Os principais indicadores de desempenho para funções críticas, como TI, segurança da informação, privacidade de dados, etc., devem ser definidos, formalmente documentados, avaliados periodicamente e relatados à alta gerência.

Segurança de rede

Obrigações do fornecedor:

26. Design de rede e arquitetura de segurança:

26.1. A rede do fornecedor deve adotar os princípios da "defesa em profundidade", incorporando controles apropriados, como segmentação de rede, para minimizar violações de informações e cibersegurança.

26.2. Um design arquitetônico sólido deve ser implementado, com um gerenciamento eficaz de identidades e configurações robustas do sistema operacional.

26.3. O design e a implementação da rede devem passar por revisões anuais para garantir eficácia e segurança contínuas.

26.4. A configuração da rede deve estar em conformidade com todos os requisitos legais e regulatórios aplicáveis.

27. Controle de acesso e autenticação:

27.1. As conexões com redes externas devem ser documentadas, roteadas por firewalls, confirmadas e aprovadas antes de serem estabelecidas.

27.2. O acesso a redes sem fio exige autenticação, autorização, segmentação e criptografia. Devem ser implementados sistemas para detectar e responder a pontos de acesso sem fio duvidosos ou conexões não autorizadas.

27.3. O acesso remoto à rede do fornecedor deve ser aprovado e realizado por meios seguros, com autenticação multifator.

27.4. Devem ser implementados controles para evitar ou minimizar o acesso não autorizado à rede do fornecedor.

28. Administração e gerenciamento seguros:

28.1. Todo o tráfego de rede relacionado a gerenciamento entre estações de trabalho administrativas e dispositivos de rede deve usar protocolos de criptografia e autenticação padrão do setor.

28.2. O acesso administrativo não realizado pelo console deve ocorrer exclusivamente por meio de canais criptografados aprovados pelo setor.

28.3. As contas de convidados devem ser desativadas ou removidas e todas as senhas padrão e fornecidas pelo fornecedor devem ser alteradas antes da implantação dos dispositivos de rede no ambiente de produção.

29. Fortalecimento da rede e proteção contra ameaças:

29.1. Os serviços, as portas e os aplicativos não usados devem ser desativados para reduzir a superfície de ataque.

29.2. Medidas de detecção e/ou prevenção de intrusões devem ser implantadas para segmentos críticos da rede.

29.3. Sistemas críticos devem ser protegidos contra ataques de Negação de Serviço (DoS) e Negação Distribuída de Serviço (DDoS).

Criptografia

Obrigações do fornecedor:

30. Uma política criptográfica abrangente, juntamente com procedimentos de apoio, deve ser implementada para garantir a conformidade com todos os requisitos legais, regulatórios e comerciais relevantes. Essa política deve seguir as melhores práticas do setor para garantir uma criptografia segura, em conformidade com as leis e as normas aplicáveis.

31. Padrões de criptografia e implementação:

31.1. Apenas algoritmos de criptografia e níveis de segurança de chave aprovados pelo setor devem ser permitidos, garantindo uma proteção adequada dos dados em todos os sistemas e processos.

31.2. Soluções criptográficas devem ser implementadas para proteger informações confidenciais e restringir o acesso a dados sigilosos, incluindo criptografia de dados em trânsito e em repouso.

31.3. O armazenamento e a transmissão de senhas devem ser criptografados, mantendo sempre a confidencialidade das credenciais de usuário.

31.4. Os dados da Alludo em trânsito devem ser criptografados, usando pelo menos o padrão TLS 1.2 ou um padrão mais recente.

31.5. Os dados da Alludo em repouso devem ser criptografados, usando pelo menos o padrão AES de 256 bits ou um padrão mais recente.

Segurança de dados

Obrigações do fornecedor:

32. Recuperação:

32.1. **Backup e recuperação de dados**:

32.1.1. Os backups de dados da Alludo devem ser realizados periodicamente.

32.1.2. Os backups de dados da Alludo devem ser mantidos por um ano.

32.1.3. Os backups de dados da Alludo devem ser criptografados.

32.2. **Recuperação de desastres**:

32.2.1. O plano de recuperação de desastres deve ser testado anualmente.

33. Procedimentos e política de backup:

33.1. A política de backup e os procedimentos de apoio devem estar claramente documentados.

33.2. Os processos de restauração de backup devem ser documentados e testados com uma frequência definida.

33.3. É necessário manter evidências dos testes de restauração de backup.

33.4. Uma cópia dos arquivos de backup de dados críticos deve ser mantida em segurança.

34. Monitoramento de backup:

34.1. Os registros de backups com falhas (se houver) devem ser monitorados pelo administrador de backups.

34.2. Ações corretivas para backups com falhas devem ser executadas e documentadas.

35. **Localização dos dados**:
    35.1. O fornecedor é responsável por garantir a conformidade com todas as leis de privacidade e proteção de dados aplicáveis nos países onde os dados serão armazenados.
    35.2. É necessário respeitar as restrições para a transferência internacional de dados (GDPR, etc.).
    35.3. O fornecedor deve implementar medidas de segurança técnicas e organizacionais apropriadas para proteger os dados, de acordo com as leis e as normas dos países onde os dados são armazenados.
    35.4. A Alludo reserva-se o direito de auditar as práticas de processamento de dados do fornecedor para garantir a conformidade com as medidas de segurança acordadas e as regulamentações locais.

36. **Exclusão de dados**:
    36.1. Devem ser implementados procedimentos para a exclusão segura de dados após a rescisão do contrato, garantindo a conformidade com as leis locais de retenção de dados.

37. **Criptografia total do disco**:
    37.1. A criptografia total do disco deve ser configurada para estações de trabalho e servidores,

38. **Classificação de dados**:
    38.1. Uma política documentada de classificação de dados deve estar em vigor.
    38.2. Os dados devem ser classificados com base em sua criticidade e em sua confidencialidade.
    38.3. Controles de segurança correspondentes à confidencialidade dos dados devem ser identificados e implementados.

Comunicação de informações

Obrigações do fornecedor:

39. **Segurança na Web**:
    39.1. Um software de filtragem de conteúdo da Web deve ser implementado para bloquear o acesso a sites que hospedam conteúdo mal-intencionado.
    39.2. Todos os sistemas e aplicativos baseados na Web devem ser acessados por meio de mecanismos seguros e autenticados.
    39.3. A comunicação cliente-servidor para aplicativos e portais da Web deve ocorrer por meio de canais criptografados.

40. **Segurança de e-mail**:
    40.1. Controles de segurança devem ser implementados para evitar o uso indevido do sistema de e-mail.
    40.2. Todas as comunicações por e-mail devem ser transmitidas por canais criptografados.
    40.3. O gateway de e-mail deve estar equipado com:
        40.3.1. Filtros anti-phishing.

40.3.2. Protocolos de segurança habilitados para e-mail (por exemplo, DMARC, DKIM e SPF).
40.3.3. Outras configurações necessárias para evitar ameaças transmitidas por e-mail.

Desenvolvimento de software

Obrigações do fornecedor:

41. **Ciclo de vida do desenvolvimento de software**:
    41.1. Uma estrutura estabelecida de desenvolvimento de software e sistemas deve ser implementada.
    41.2. Os sistemas e os aplicativos devem ser desenvolvidos seguindo as melhores práticas de desenvolvimento seguro de software (por exemplo, OWASP).
    41.3. O código de software deve ser:
        41.3.1. Protegido contra modificações não autorizadas
        41.3.2. Armazenado com segurança
        41.3.3. Submetido a processos de garantia de qualidade
    41.4. Revisões de código devem ser realizadas.

42. **Testes e implantação**:
    42.1. Os aplicativos devem passar por testes completos de segurança e funcionalidade antes da implantação no ambiente de produção.
    42.2. Os ambientes de produção e de não produção devem estar devidamente segregados.
    42.3. A segregação de funções entre desenvolvimento para produção e não produção deve ser mantida.
    42.4. Não devem existir dados de produção em um ambiente de teste.

Segurança de aplicativos

Obrigações do fornecedor:

43. **Segurança de aplicativos:**
    43.1. Avaliações de segurança de aplicativos devem ser realizadas para todos os aplicativos recém-desenvolvidos e para quaisquer aplicativos existentes que passem por alterações significativas, a fim de identificar vulnerabilidades de segurança conhecidas.
    43.2. Todas as vulnerabilidades de segurança identificadas com uma pontuação CVSS superior a 4 devem ser atenuadas antes da implantação do aplicativo no ambiente de produção.
    43.3. Processos de revisão de código devem ser implementados para identificar e corrigir códigos que possam introduzir vulnerabilidades de segurança.

44. **Proteção de aplicativos Web:**
    44.1. Os aplicativos Web voltados para o público devem estar protegidos por um robusto firewall de aplicativos Web para evitar ameaças externas.

Gerenciamento de patches

Obrigações do fornecedor:

45. Os patches de segurança mais recentes devem ser aplicados a sistemas, redes, aplicativos, bancos de dados etc. em tempo hábil e com base na criticidade da vulnerabilidade resolvida pelo patch. Os patches são obtidos diretamente dos respectivos OEMs para sistemas proprietários.

46. Todos os patches devem ser testados antes da sua implantação nos sistemas de produção e a operação correta do serviço que recebeu o patch deve ser confirmada após qualquer atividade de aplicação de patches.

47. Atenuações apropriadas deverão ser implementadas caso não seja possível aplicar patches a um sistema. A eficácia dessas atenuações deve ser avaliada periodicamente e as evidências correspondentes devem ser mantidas.

Proteção contra malware

Obrigações do fornecedor:

48. Todos os sistemas de TI devem estar continuamente protegidos por uma solução de proteção contra malware que inspecione os dados recebidos em tempo real para evitar interrupções de serviço ou violações de segurança. Além disso, procedimentos adequados de conscientização do usuário devem ser aplicados. O sistema anti-malware deve detectar várias ameaças, incluindo entre outras: vírus, spyware, worms, códigos móveis não autorizados, keyloggers, botnets e cavalos de Troia.

49. As assinaturas de malware devem ser atualizadas regularmente para garantir que os sistemas estejam sempre equipados com as definições de ameaças mais recentes.

50. O software de proteção contra malware deve estar configurado para executar verificações programadas e sob demanda e para isolar ou excluir qualquer arquivo ou software mal-intencionado identificado.

51. Os usuários finais não devem ter o direito ou a capacidade de desativar a proteção contra malware.

Gerenciamento de vulnerabilidades

Obrigações do fornecedor:

52. Processo de gerenciamento de vulnerabilidades:

52.1. Políticas, processos e procedimentos estabelecidos para um gerenciamento abrangente de vulnerabilidades.

52.2. Processos para receber, analisar e responder a vulnerabilidades de fontes internas e externas.

53. Avaliação e correção de vulnerabilidades:

53.1. Avaliações trimestrais de vulnerabilidades na infraestrutura de TI e nos aplicativos do fornecedor, incluindo sites de recuperação de desastres.

53.2. Correção de vulnerabilidades identificadas com pontuação CVSS superior a 4 dentro dos prazos definidos.

54. Testes de penetração:

54.1. Testes de penetração independentes anuais na infraestrutura de TI e nos aplicativos do fornecedor usados para serviços da Alludo.

54.2. Os testes visam identificar vulnerabilidades exploráveis e evitar violações de segurança por meio de ciberataques.

54.3. A Alludo deverá ter acesso aos relatórios relevantes de testes de penetração/vulnerabilidade mediante solicitação razoável.

Registro e monitoramento

Obrigações do fornecedor:

55. Sistemas críticos, incluindo aplicativos, devem estar configurados para registrar os principais eventos (incluindo aqueles de acesso privilegiado e atividade do usuário) e retê-los por um período mínimo de 1 ano ou conforme os requisitos regulatórios aplicáveis.

56. Os registros dos principais eventos (quando aplicável) devem conter, no mínimo, o seguinte:

56.1. Inicialização e desligamento do sistema.

56.2. Status de início e parada de serviços e processos críticos.

56.3. Alterações no parâmetro de configuração, por exemplo, alterações na configuração de inicialização do sistema.

56.4. Logins bem-sucedidos e tentativas de login malsucedidas.

56.5. Criação, modificação e exclusão de contas de usuário.

56.6. Sistema/recursos acessados.

56.7. Identificação e localização de quem acessou os recursos e de onde.

56.8. Data e hora.

57. Os registros de auditoria devem ser coletados em vários sensores e fontes, correlacionados e armazenados de forma segura e devem ser antifalsificação para permitir a reconstrução de tais eventos.

58. Processos para monitorar eventos de registro (de preferência em tempo real) devem ser estabelecidos para detectar atividades não autorizadas e alvos de ataque e para garantir que os registros dos principais eventos sejam revisados.

Gerenciamento de incidentes

Obrigações do fornecedor:

59. As funções e os processos devem ser claramente definidos para garantir uma resposta rápida, eficaz e organizada aos incidentes de privacidade e segurança da informação.

60. Os funcionários e os prestadores de serviços devem ser treinados para reconhecer o que constitui um incidente de segurança e também como e onde relatar quaisquer incidentes potenciais ou confirmados.

61. O pessoal responsável por analisar e responder a incidentes deve ser qualificado no assunto e passar por treinamento regular sobre práticas eficazes de resposta a incidentes.

62. Um repositório deve ser mantido para todos os incidentes relatados, detalhando as ações adotadas para atenuar o impacto do incidente e as lições aprendidas com o evento.

63. A Alludo deve ser notificada assim que a organização tomar conhecimento de qualquer incidente de segurança que a afete, mas em até 24 horas depois da detecção.

Segurança física e ambiental

Obrigações do fornecedor:

64. Devem ser implementados procedimentos e políticas para segurança física e controles ambientais, alinhados com as normas do setor.
65. Instalações críticas que abrigam sistemas de TI, aplicativos e pessoal (por exemplo, centros de dados, sites operacionais) devem estar protegidas contra acidentes, ataques e acessos não autorizados.
66. Medidas de segurança, como controles eletrônicos de acesso, confirmação de identidade, seguranças, gerenciamento de visitantes e monitoramento ininterrupto por CFTV, devem estar implementadas para impedir a entrada não autorizada.
67. As imagens de CFTV devem ser retidas por pelo menos 30 dias, ou mais, se exigido por regulamentações legais.
68. O acesso às instalações deve ser restrito a pessoal autorizado para fins específicos e deve ser revisado regularmente.
69. Os visitantes devem ser acompanhados, seus horários de entrada e saída devem ser registrados e eles devem usar identificações de visitante o tempo todo. As chaves ou os cartões de acesso devem ser recolhidos no momento da saída.
70. As instalações críticas devem estar protegidas contra perda de energia usando fontes de alimentação ininterrupta (UPS) ou geradores para garantir operações contínuas.
71. Uma manutenção periódica deve ser realizada em equipamentos críticos, como UPS, geradores, detectores de fumaça, sistemas de supressão de incêndio e sistemas de controle de acesso, com os registros devidamente mantidos.
72. As instalações devem ser construídas com materiais à prova de fogo e estar equipadas com alarmes de incêndio, detectores de fumaça, sensores de temperatura e de inundação, além de extintores de incêndio, para proteção contra riscos naturais.
73. Devem ser definidos mecanismos de descarte seguro para dados, tanto em formatos físicos quanto digitais, usando fragmentadoras de corte transversal para papel e métodos como sanitização, desmagnetização ou destruição para mídia eletrônica.
74. Uma política de mesa limpa garante o manuseio seguro de post-its, documentos escritos e mídias removíveis.
75. Controles físicos e ambientais devem ser avaliados quanto à eficácia pelo menos uma vez por ano.

Privacidade e proteção de dados

Se o fornecedor ou seus subprocessadores processarem dados pessoais em nome da Alludo ou dos clientes da Alludo, o fornecedor deverá garantir o seguinte:

76. **Governança e conformidade com a privacidade de dados:**

76.1. Cumprimento de todas as leis aplicáveis de proteção de dados.
76.2. Estabelecimento de uma estrutura de gerenciamento de privacidade incluindo:
76.3. Políticas, declarações, avisos e procedimentos de privacidade (revisados anualmente).
76.4. Processos de gerenciamento de riscos e governança de privacidade.
76.5. Cumprimento de requisitos legais e regulatórios.
76.6. Manutenção de registros atualizados das atividades de processamento dos dados pessoais da Alludo.
76.7. Definição e implementação de funções e responsabilidades apropriadas para privacidade de dados:
76.8. Nomeação de um diretor de privacidade de dados (ou equivalente).
76.9. Estabelecimento de uma função especializada em privacidade de dados.
76.10. Formação de um comitê para coordenar as atividades de conformidade com a privacidade de dados.

77. Medidas de proteção e segurança de dados

77.1. Implementar mecanismos de proteção padrão do setor (por exemplo, ISO/IEC 27001:2013, SOC2, etc.) para
proteger as informações da Alludo.
77.2. Aplicar outros mecanismos de proteção para dados pessoais confidenciais (por exemplo, criptografia, pseudonimização).
77.3. Aplicar controles de acesso:
77.4. Restringir o acesso com base na necessidade e no princípio do menor privilégio.
77.5. Remover os direitos de acesso imediatamente após o término do contrato ou mudanças de função.
77.6. Realizar revisões periódicas dos direitos de acesso.
77.7. Garantir compromissos de confidencialidade de todo o pessoal que processa dados pessoais.

78. Gerenciamento de direitos de titular de dados:

78.1. Ajudar a Alludo a cumprir as obrigações relacionadas aos direitos de titular de dados.
78.2. Notificar a Alludo em até dois dias após o recebimento de solicitações de titulares de dados.
78.3. Responder às solicitações apenas conforme as instruções da Alludo, a menos que haja exigência legal em contrário.

79. Resposta a incidentes:

79.1. Notificar a Alludo em até 24 horas sobre violações de dados pessoais envolvendo dados da Alludo.

Medidas de subcontratação

Obrigações do fornecedor:

80. Garantir a realização de avaliações anuais de riscos de terceiros em todos os subprocessadores envolvidos no manuseio, no processamento ou no armazenamento de dados da Alludo. Essas avaliações devem analisar os controles de segurança dos subprocessadores, as medidas de proteção de dados, a conformidade com as regulamentações relevantes e a postura geral de risco. Os fornecedores devem apresentar a documentação dessas avaliações mediante solicitação, resolver prontamente quaisquer riscos identificados e comunicar quaisquer mudanças nos subprocessadores ou descobertas significativas em tempo hábil. Reservamo-nos o direito de revisar os resultados da avaliação e de solicitar medidas de segurança adicionais, se necessário.

Gerenciamento de continuidade dos negócios

Obrigações do fornecedor:

81. Uma política de gerenciamento de continuidade dos negócios (BCM) deve ser estabelecida, acompanhada de planos e procedimentos detalhados. Esses documentos devem descrever os objetivos de continuidade dos negócios da organização e passar por revisão e aprovação anuais.

82. Uma estrutura de testes de BCM deve ser desenvolvida e implementada para avaliar a eficácia das estratégias de continuidade dos negócios existentes.

83. As análises de impacto nos negócios (BIA) devem ser conduzidas pelo menos uma vez por ano ou após mudanças organizacionais significativas.

84. Um plano de gerenciamento de crise deve ser estabelecido, incluindo disposições específicas relativas à preparação para pandemias. Esse plano deve garantir uma resposta adequada a emergências, com foco na proteção dos funcionários, dos visitantes, do meio ambiente e dos ativos e na manutenção de operações comerciais críticas.

85. O sistema de gerenciamento de continuidade dos negócios (BCMS) deve passar por testes anuais de eficácia, sendo mantidos registros detalhados para cada teste.

<Fim do documento>