RESUMO DAS MEDIDAS DE SEGURANÇA DA HP

Com o intuito de proteger os dados do Cliente, a HP cumpre um conjunto sólido de controlos de segurança de informações, que inclui políticas, práticas, procedimentos e estruturas organizacionais para salvaguardar a confidencialidade, integridade e disponibilidade, quer das suas próprias informações, quer das informações dos clientes (incluindo Dados Pessoais, tal como definido na Adenda de Processamento de Dados do Cliente da HP). Apresentamos a seguir uma descrição geral das medidas de segurança técnicas/organizacionais da HP em toda a empresa.

1. Política de Segurança

   Em termos globais, a HP mantém políticas, normas e procedimentos aplicáveis que se destinam a proteger os dados da HP e do Cliente. Os detalhes das políticas de segurança da HP são confidenciais, de modo a proteger a integridade dos dados e sistemas da HP. No entanto, os resumos das nossas principais políticas são apresentados abaixo.

2. Organização da Segurança de Informações

   O programa de Segurança de Informações da HP foi criado para orientar e manter a estratégia e os controlos de segurança de informações da organização. O sistema assegura a conformidade empresarial com as políticas e controlos de segurança da HP, bem como a adesão aos requisitos de segurança dos respetivos clientes. Estruturado em alinhamento com os âmbitos, leis e regulamentos de cibersegurança normativos do setor, o Enquadramento é revisto anualmente para se adaptar ao crescente cenário da ameaças da HP.

3. Gestão de Riscos Cibernéticos

   O programa de gestão de riscos cibernéticos da HP foi concebido para preservar a confidencialidade, integridade e disponibilidade dos respetivos recursos de informação. O programa oferece uma abordagem consistente para identificar, avaliar, priorizar, tratar, solucionar, acompanhar e denunciar riscos cibernéticos. A HP define a sua Apetência pelo Risco como nível aceitável de exposição à perda e Tolerância ao Risco como grau de variação desta apetência. Os riscos são avaliados através de uma metodologia definida, permitindo à HP mitigar riscos de segurança de informações a um nível aceitável. Este programa está alinhado com o processo de Gestão de Riscos Empresariais da HP.

4. Segurança de RH

   A política de Segurança de Recursos Humanos da HP garante a segurança das informações durante o ciclo de vida do colaborador, ao estabelecer processos de acesso às instalações, sistemas de informação e outros recursos. Isto implica a obtenção de reconhecimentos por escrito através de acordos de confidencialidade e não divulgação, bem como a orientação de procedimentos de verificação em segundo plano. Todos os candidatos admitidos pela HP têm de concluir uma verificação de antecedentes, de acordo com as leis, regulamentos e ética relevantes.

5. Gestão de Recursos

   A HP dispõe de um processo para identificar recursos de informações técnicas, categorizar ativos críticos e efetuar a manutenção de procedimentos de tratamentos documentados para cada tipo de classificação de informação, incluindo os que contêm Dados Pessoais. Estes procedimentos abrangem o armazenamento, transmissão, comunicação, acesso, início de sessão, retenção, destruição, eliminação, gestão de incidentes e notificação de violações. As políticas e normas de segurança da HP autorizam igualmente a eliminação segura dos ficheiros multimédia.

6. Segurança de Dados

   O programa de Segurança de Dados da HP descreve as práticas e controlos técnicos de segurança que têm de ser implementados para proteger a confidencialidade, autenticidade e integridade dos dados. Requisitos legais, valor, criticidade e sensibilidade à divulgação não autorizada ou modificação são apenas alguns dos fatores que determinam o modo como as informações são classificadas de acordo com a política de Segurança de Dados da HP. Além dos procedimentos de tratamento de dados, a política descreve a encriptação, eliminação, recolha e processamento, retenção, cópia de segurança dos dados e prevenção contra a perda de dados.

7. Controlo de Acessos

   A HP utiliza o princípio do privilégio mínimo para o controlo de acessos lógico, fornecendo ao utilizador acesso através de IDs e palavras-passe exclusivos. A política de palavras-passe define a complexidade, solidez, validade e controlos de histórico de palavras-passe. Os direitos de acesso são revistos e revogados periodicamente após a saída dos colaboradores. Os procedimentos acordados para a criação e eliminação de contas são implementados para conceder e revogar o acesso aos sistemas de clientes durante as interações.

8. Criptografia

   A HP definiu um conjunto de processos robustos a nível de criptografia para assegurar a confidencialidade, integridade e disponibilidade dos recursos de informação. Os protocolos aprovados requerem encriptação para determinados recursos, incluindo aqueles que contêm dados pessoais. O nosso programa de Criptografia envolve a utilização de técnicas matemáticas para proteger as informações e as comunicações, assegurando que apenas as partes autorizadas conseguem aceder aos dados. Um componente crítico do programa de informação da HP é proteger os dados do acesso não autorizado e da adulteração.

9. Segurança Física e Ambiental

   As instalações da HP estão protegidas através de diversos controlos físicos e eletrónicos, incluindo pessoal da segurança, controlo de acesso eletrónico e televisão em circuito fechado (CCTV). As instalações também estão equipadas com o apoio de infraestrutura necessário, incluindo controlo de temperatura e sistema de alimentação de reserva, utilização de UPS e/ou geradores a diesel para dar apoio a serviços críticos. Todos os colaboradores da HP estão registados e têm de usar os respetivos cartões de identificação.

10. Gestão de Operações

    A HP estabeleceu requisitos mínimos reforçados para a infraestrutura tecnológica, incluindo estações de trabalho, servidores e equipamento de rede. Estes dispositivos utilizam imagens do sistema operativo pré-reforçados, com requisitos que variam por sistema operativo e controlos implementados. Adicionalmente, a HP desenvolveu Sistemas de Deteção/Prevenção de Intrusão na Rede (NIDS/NIPS) que são monitorizados e geridos 24 horas por dia, 7 dias por semana.

11. Segurança das Comunicações

    A Segurança das Comunicações garante a proteção das informações nas redes empresariais. Isto inclui a instalação e gestão de componentes de segurança da rede (por ex. firewalls), a segregação de redes, bem como a filtragem da web e controlos de tratamento de e-mails. Além disso, envolve a monitorização e gestão dos canais de comunicação para detetar e impedir o acesso não autorização ou violações dos dados.

12. Segurança dos Sistemas

    A política da HP exige uma metodologia de desenvolvimento segura para sistemas e software ao longo dos respetivo ciclo de vida. O Ciclo de Vida de Desenvolvimento do Software abrange a iniciação, desenvolvimento/aquisição, implementação, operações e eliminação. Todos os componentes de sistema são avaliados a nível do respetivo impacto na segurança em geral. A HP estabeleceu controlos para transações de serviço do aplicações, incluindo validação de credenciais do utilizador, assinaturas digitais, encriptação, protocolos de comunicação segura e armazenamento de detalhes de transações na zona de segurança de rede adequada. São igualmente realizadas verificações de vulnerabilidade internas periódicas.

13. Terceiros e subcontratantes

    A HP dispõe de processos para selecionar subcontratantes que cumpram requisitos de segurança contratuais abrangentes. No caso de fornecedores aplicáveis que fazem o tratamento de dados da HP ou de clientes ou que acedem à rede da HP, a Cibersegurança da HP realiza uma avaliação dos riscos para verificar um programa de segurança de informação com salvaguardas físicas, técnicas e administrativas. Esta avaliação é obrigatória antes de o fornecedor conseguir ter acesso às informações da HP.

14. Gestão de Incidentes de Segurança de Informação

    A HP dispõe de um Processo de Gestão de Incidentes Cibernéticos abrangentes que descreve a finalidade, âmbito, funções, responsabilidades, compromisso de gestão, coordenação organizacional, procedimentos de implementação e verificação da conformidade. Este processo é revisto e atualizado anualmente. A Equipa de Resposta a Incidentes Cibernéticos, que inclui colaboradores de Cibersegurança da HP formado em gestão de crises e resposta a incidentes, realiza revisões avançadas regulares do processo e quaisquer incidentes ou eventos.

15. Gestão de Continuidade Comercial

    O programa global de Continuidade de Operações da HP assegura a continuidade completa através de processos de planeamento colaborativo, padronizado e documentado. A empresa realiza periodicamente os respetivos planos de continuidade comercial para garantir a eficácia, testes e atualização de todos os planos, no mínimo, anualmente. Além disso, todos os colaboradores envolvidos no plano de continuidade comercial recebem formação adequada.

16. Conformidade

    A conformidade define a abordagem da HP em cumprir as expetativas jurídicas, contratuais e internas para um programa de segurança de informação eficaz. As revisões de segurança de informação regulares garantem que os protocolos são integrados em cada uma das operações do grupo empresarial. O processo de revisão também mantém os documentos atualizados para refletir as obrigações jurídicas atuais à medida que os requisitos evoluem.

17. Setor de Cartões de Pagamento

    A estrutura do Setor de Cartões de Pagamento (PCI) orienta a abordagem da HP para alcançar a Conformidade do PCI, descrevendo as responsabilidade da empresa e os controlos de segurança alinhados com o PCI DSS. Ao instalar e manter os controlos de segurança da rede, como as firewalls, a HP assegura o cumprimento dos requisitos de Conformidade do PCI.

18. Segurança de Produtos HP

    A Segurança de Produtos HP engloba práticas essenciais para proteger os Produtos HP, tais como assinatura de código, gestão de vulnerabilidades de segurança de produtos, emissão de boletins de segurança e comunicação de problemas de segurança de produtos. Estas medidas garantem que os produtos da HP continuam seguros e fiáveis para os utilizadores. A segurança dos produtos é de uma importância primordial na HP, uma vez que ajuda a manter a confiança do cliente e a proteger contra potenciais ameaças.

19. Segurança dos Serviços HP

    A Segurança dos Serviços HP engloba práticas essenciais para proteger os serviços fornecidos aos clientes da HP. Esta política aborda várias áreas da segurança dos serviços, incluindo os ambientes alojados da infraestrutura da HP, ambientes alojados de terceiros, ambientes alojados de parceiros e ambientes alojados de clientes. Estas medidas asseguram que esses serviços da HP continuam seguros e fiáveis para os utilizadores. Ao implementar práticas de segurança robustas, a HP garante a segurança e a integridade dos respetivos produtos e serviços, promovendo um ambiente protegido e fidedigno para todos os utilizadores.