RESUMO DAS MEDIDAS DE SEGURANÇA DA HP

Para proteger os dados do cliente, a HP respeita um conjunto robusto de controles de segurança da informação, incluindo políticas, práticas, procedimentos e estruturas organizacionais para proteger o sigilo, a integridade e a disponibilidade de suas próprias informações e das informações dos clientes (incluindo Dados pessoais, conforme definido no Adendo de processamento de dados e clientes da HP). Os itens a seguir definem uma visão geral das medidas de segurança técnica/organizacional da HP em toda a empresa.

1. Política de segurança

   A HP mantém políticas, padrões e procedimentos aplicáveis globalmente com o objetivo de proteger os dados da HP e do cliente. Os detalhes das políticas de segurança da HP são confidenciais para proteger a integridade dos dados e sistemas da HP. No entanto, resumos de nossas principais políticas estão incluídos abaixo.

2. Organização de segurança da informação

   O programa de Segurança da informação da HP foi projetado para direcionar e manter a estratégia e os controles de segurança da informação da organização. Esse sistema garante a conformidade em toda a empresa com as políticas e os controles de segurança da HP, bem como a adesão aos requisitos de segurança dos clientes. Estruturado de acordo com estruturas, leis e regulamentos de segurança cibernética padrão do setor, a estrutura é revisada anualmente para se adaptar ao cenário de ameaças em evolução da HP.

3. Gerenciamento de riscos de segurança cibernética

   O programa de gerenciamento de riscos de segurança cibernética da HP foi projetado para preservar a confidencialidade, a integridade e a disponibilidade dos ativos de informação. O programa fornece uma abordagem consistente para identificar, avaliar, priorizar, tratar, sanar, controlar e relatar riscos de segurança cibernética. A HP define seu Apetite por Risco como o nível aceitável de exposição a perdas e Tolerância ao Risco como o grau de variação desse apetite. Os riscos são avaliados usando uma metodologia definida, permitindo que a HP diminua os riscos de segurança da informação a um nível aceitável. Esse programa está alinhado com o processo de gerenciamento de riscos empresariais da HP.

4. Segurança do RH

   A política de Segurança de recursos humanos da HP garante a segurança da informação em todo o ciclo de vida dos funcionários, estabelecendo processos para acesso a instalações, sistemas de informações e outros dispositivos. Isso inclui a obtenção de reconhecimentos por escrito por meio de acordos de confidencialidade e não divulgação, bem como a realização de procedimentos de triagem de antecedentes. Todos os candidatos a uma vaga na HP devem concluir uma verificação de histórico de acordo com leis, regulamentos e ética relevantes.

5. Gerenciamento de ativos

   A HP possui um processo para identificar ativos de informações técnicas, classificar ativos críticos e manter procedimentos documentados de manuseio para cada tipo de classificação de informações, incluindo os que contêm Dados pessoais. Esses procedimentos abrangem armazenamento, transmissão, comunicação, acesso, registro, retenção, destruição, descarte, gerenciamento de incidentes e notificação de violação. As políticas e os padrões de segurança da HP também obrigam o descarte seguro de mídia.

6. Segurança de dados

   O programa de segurança de dados da HP descreve as práticas de segurança e os controles técnicos que devem ser implementados para proteger a confidencialidade, a autenticidade e a integridade dos dados. Requisitos legais, valor, importância e sensibilidade à divulgação ou modificação não autorizada são alguns dos fatores que determinam como as informações são classificadas sob a política de Segurança de dados da HP. Além dos procedimentos de manuseio de dados, a política descreve criptografia de dados, exclusão, coleta e processamento, retenção, backup e prevenção de perda de dados.

7. Controle de acesso

   A HP utiliza o princípio de privilégio mínimo para controle de acesso lógico, fornecendo acesso ao usuário por meio de IDs e senhas exclusivos do usuário. A política de senha define controles de complexidade, força, validade e histórico de senhas. Os direitos de acesso são revisados periodicamente e revogados após a saída dos funcionários. Os procedimentos acordados para criação e exclusão de conta de usuário são implementados para conceder e revogar acesso aos sistemas cliente durante os compromissos.

8. Criptografia

   A HP definiu um conjunto de processos robustos para criptografia que garantem a confidencialidade, a integridade e a disponibilidade dos ativos de informação. Os protocolos aprovados exigem criptografia para determinados dispositivos, incluindo aqueles que contêm dados pessoais. Nosso programa de criptografia envolve o uso de técnicas matemáticas para proteger informações e comunicações, garantindo que apenas partes autorizadas possam acessar os dados. Um componente essencial do programa de segurança da informação da HP é a proteção dos dados contra o acesso não autorizado e a violação.

9. Segurança física e ambiental

   As instalações da HP são protegidas por meio de vários controles de acesso físico e eletrônico, incluindo seguranças, controle de acesso eletrônico e Circuito fechado de televisão (CFTV). As instalações também estão equipadas com o suporte necessário à infraestrutura, incluindo controle de temperatura e backups de energia, usando UPS e/ou geradores a diesel para suportar serviços essenciais. Todos os funcionários da HP são registrados e devem levar distintivos de identificação apropriados.

10. Gerenciamento de operações

    A HP estabeleceu requisitos mínimos de reforço da infraestrutura de tecnologia, incluindo estações de trabalho, servidores e equipamentos de rede. Esses dispositivos usam imagens previamente protegidas do sistema operacional, com requisitos que variam de acordo com o sistema operacional e controles implementados. Além disso, a HP implantou sistemas de detecção/prevenção de intrusão de rede (NIDS/NIPS) que são monitorados e gerenciados 24 horas por dia, 7 dias por semana.

11. Segurança de comunicações

    A segurança de comunicações garante a proteção das informações nas redes corporativas. Isso inclui a instalação e o gerenciamento de componentes de segurança de rede (por exemplo, firewalls), segregação de redes, bem como controles de filtragem da Web e manuseio de e-mail. Além disso, envolve o monitoramento e o gerenciamento de canais de comunicação para detectar e evitar acesso não autorizado ou violações de dados.

12. Segurança de sistemas

    A política da HP exige uma metodologia de desenvolvimento segura para sistemas e software durante todo o ciclo de vida. O ciclo de vida de desenvolvimento do software abrange iniciação, desenvolvimento/aquisição, implementação, operações e descarte. Todos os componentes do sistema são avaliados pelo seu impacto na segurança geral. A HP estabeleceu controles para transações de serviço de aplicativo, incluindo validação de credencial de usuário, assinaturas digitais, criptografia, protocolos de comunicação segura e armazenamento de detalhes de transação dentro da zona de segurança de rede apropriada. Verificações regulares de vulnerabilidade interna também são executadas.

13. Terceiros e subcontratados

    A HP tem processos para selecionar subcontratados que satisfaçam requisitos abrangentes de segurança contratual. Para fornecedores aplicáveis que manuseiam dados da HP ou de clientes ou acessam a rede HP, o HP Cybersecurity realiza uma avaliação de risco para verificar um programa de segurança da informação com proteções físicas, técnicas e administrativas. Essa avaliação é necessária para que o fornecedor possa acessar as informações da HP.

14. Gerenciamento de incidentes de segurança da informação

    A HP possui um abrangente processo de gerenciamento de incidentes cibernéticos que descreve propósito, escopo, funções, responsabilidades, compromisso de gerenciamento, coordenação organizacional, procedimentos de implementação e verificação de conformidade. Esse processo é revisado e atualizado anualmente. A Equipe de Resposta a Incidentes Cibernéticos, incluindo a equipe de Segurança Cibernética da HP treinada em resposta a incidentes e gerenciamento de crises, realiza revisões regulares sobre o processo e quaisquer incidentes ou eventos.

15. Gerenciamento de continuidade de negócios

    O programa global de Continuidade de Operações da HP garante continuidade de ponta a ponta por meio de processos colaborativos, padronizados e documentados de planejamento. A empresa exerce periodicamente seus planos de continuidade de negócios para garantir eficiência, testando e atualizando todos os planos pelo menos anualmente. Além disso, todos os funcionários envolvidos no plano de continuidade de negócios recebem um treinamento adequado.

16. Conformidade

    A conformidade molda a abordagem da HP para atender às expectativas legais, contratuais e internas de um programa eficaz de segurança da informação. Revisões regulares de segurança da informação garantem que os protocolos estejam integrados às operações de cada grupo de negócios. O processo de revisão também mantém documentos atualizados para refletir as obrigações legais atuais conforme os requisitos evoluem.

17. Setor de cartões de pagamento

    A estrutura do Indústria de cartões de pagamento (PCI) orienta a abordagem da HP para alcançar a conformidade com o PCI, delineando responsabilidades comerciais e controles de segurança alinhados com o PCI-DSS. Ao instalar e manter controles de segurança de rede como firewalls, a HP garante que satisfaz os requisitos de conformidade com o PCI.

18. Segurança do produto da HP

    A Segurança do produto da HP engloba práticas essenciais para proteger produtos da HP, como assinar códigos, gerenciar vulnerabilidades de segurança do produto, emitir boletins de segurança e relatar problemas de segurança do produto. Essas medidas garantem que os produtos da HP permaneçam seguros e confiáveis para os usuários. A segurança do produto é de suma importância para a HP, pois ajuda a manter a confiança do cliente e a se proteger contra possíveis ameaças.

19. Segurança de serviços da HP

    A Segurança de serviços da HP engloba práticas essenciais para proteger os serviços fornecidos aos clientes da HP. Essa política aborda várias áreas de segurança de serviços, incluindo ambientes hospedados em infraestrutura da HP, hospedados por terceiros, hospedados por parceiros e ambientes hospedados por clientes. Essas medidas garantem que os serviços da HP permaneçam seguros e confiáveis para os usuários. Ao implementar práticas robustas de segurança, a HP garante a segurança e a integridade de seus produtos e serviços, promovendo um ambiente seguro e confiável para todos os usuários.