SÍNTESE DAS MEDIDAS DE SEGURANÇA DA HP

---

Para proteger os dados dos Clientes, a HP cumpre um conjunto robusto de controlos de segurança da informação, incluindo políticas, práticas, procedimentos e estruturas organizacionais para salvaguardar a confidencialidade, integridade e disponibilidade das suas próprias informações e das informações dos seus clientes (incluindo Dados Pessoais, tal como definido nas Adendas ao Tratamento de Dados e Cliente da HP). A seguir, é apresentada uma visão geral das medidas de segurança técnica/organizacional da HP em toda a empresa.

1. Política de segurança

A HP mantém políticas, normas e procedimentos globalmente aplicáveis destinados a 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 dos sistemas da HP. No entanto, apresentamos de seguida uma síntese das nossas principais políticas.

2. Organização de segurança da informação

A HP tem uma Organização de Segurança da Informação responsável por dirigir e gerir a estratégia e os controlos de segurança da informação da organização. É implementado um Quadro de Segurança/Sistema de Gestão da Informação para garantir a conformidade com as políticas e controlos de segurança da HP e confirmar que os requisitos de segurança dos seus clientes são cumpridos. Este quadro está estruturado de acordo com o NIST Cybersecurity Framework e é revisto anualmente.

3. Gestão de ativos

A HP dispõe de um processo para identificar os ativos das informações técnicas e, através desse processo, identifica todos os ativos pelos quais são responsáveis e categoriza os ativos críticos. A HP mantém ainda um conjunto de procedimentos de tratamento documentados para cada tipo de classificação de informações, incluindo os ativos que contêm Dados Pessoais. Os procedimentos de tratamento abordam armazenamento, transmissão, comunicação, acesso, registo, retenção, destruição, eliminação, gestão de incidentes e notificação de violações.

4. Controlo de acesso

O princípio do menor privilégio é utilizado para fornecer o controlo do acesso lógico. O acesso do utilizador é fornecido através de um ID e de uma palavra-passe únicos. A política de palavras-passe da HP definiu controlos relacionados com a complexidade, força, validade e histórico de palavras-passe. Os direitos de acesso são revistos periodicamente e revogados aquando da saída do pessoal.

Os procedimentos de criação e eliminação das contas de utilizador, mutuamente acordados, são

implementados para conceder e revogar o acesso aos sistemas do cliente utilizados durante a contratação.

5. Formação do pessoal

Os colaboradores da HP têm de concluir a formação designada Integridade na HP, concebida para garantir que os colaboradores estão familiarizados com o programa, as políticas e os recursos que regem as expectativas da HP em termos de comportamento ético, excelência e conformidade. A Integridade da HP inclui módulos sobre segurança e privacidade de dados, e os colaboradores também são obrigados a frequentar um curso anual de revisão dos mesmos. Os colaboradores da HP também têm de concluir uma formação de sensibilização para a segurança, atualizada anualmente, centrada nas políticas de segurança essenciais e nas responsabilidades dos colaboradores relacionadas com a gestão de incidentes, a privacidade dos dados e a segurança das informações.

6. Terceiros e subcontratantes ulteriores

A HP tem processos em vigor para selecionar subcontratantes ulteriores capazes de cumprir os requisitos de segurança contratuais abrangentes.

Para os fornecedores aplicáveis (fornecedores que lidam/armazenam/transmitem dados da HP e dados detidos pela HP pertencentes a clientes ou que têm acesso à rede da HP), a HP Cybersecurity efetua uma avaliação de risco para verificar a existência de um programa de segurança da informação. Um programa adequado deve incluir salvaguardas físicas, técnicas e administrativas. Esta avaliação deve ser efetuada antes de o fornecedor ter acesso às informações da HP.

7. Segurança de sistemas

Segundo a política, o desenvolvimento de sistemas e software de apoio na HP segue uma metodologia de desenvolvimento seguro para garantir a segurança ao longo do ciclo de vida do sistema/software. O ciclo de vida de desenvolvimento de software define os requisitos de iniciação, desenvolvimento/aquisição, implementação, operações e eliminação. Todos os componentes do sistema, incluindo módulos, bibliotecas, serviços e componentes discretos, são avaliados para determinar o seu impacto no estado geral da segurança do sistema.

A HP definiu controlos para a proteção das transações de serviços de aplicação. Estes controlos incluem a validação e verificação das credenciais dos utilizadores, a obrigatoriedade de assinaturas digitais e encriptação, a implementação de protocolos de comunicação seguros e o armazenamento dos dados das transações online em servidores dentro da zona de segurança de rede adequada.

As verificações de vulnerabilidade interna são efetuadas com regularidade.

8. Segurança física e ambiental

As instalações da HP estão protegidas com vários controlos de acesso físico e eletrónico e recursos de vigilância. Dependendo da instalação, isto pode incluir seguranças, controlo de acesso eletrónico e televisão em circuito fechado (CCTV).

Todos os colaboradores da HP estão registados e têm de usar os distintivos de identificação apropriados.

Sempre que necessário, as instalações dispõem das infraestruturas de apoio necessárias, com controlo da temperatura e reservas de energia, utilizando UPS e/ou geradores a diesel para apoiar os serviços críticos.

## 9. Gestão de operações

A HP definiu um conjunto mínimo de requisitos de reforço para a infraestrutura tecnológica, incluindo estações de trabalho, servidores e equipamento de rede. As imagens das estações de trabalho/servidores contêm sistemas operativos previamente reforçados. Os requisitos de reforço variam consoante o tipo de sistema operativo e os controlos aplicáveis implementados.

A HP implementou Sistemas de Deteção/Prevenção de Intrusões na Rede (NIDS/NIPS) na rede, que são monitorizados e geridos 24 horas por dia, 7 dias por semana.

As políticas e normas de segurança da HP exigem a eliminação segura de suportes.

## 10. Criptografia

A HP definiu um conjunto de processos robustos de criptografia para garantir a confidencialidade, integridade e disponibilidade dos ativos de informação. Os protocolos aprovados requerem encriptação para determinados ativos, incluindo aqueles que contêm dados pessoais.

## 11. Gestão de incidentes de segurança da informação

A HP segue um Processo de Gestão de Incidentes Cibernéticos que aborda o objetivo, âmbito, funções, responsabilidades, compromisso de gestão, coordenação organizacional, procedimentos de implementação e verificação de conformidade. A HP revê e atualiza este processo todos os anos.

Uma Equipa de Resposta a Incidentes Cibernéticos, que inclui o pessoal da HP Cybersecurity com formação em resposta a incidentes e gestão de crises, é reunida para análises regulares do processo e de qualquer incidente ou acontecimento.

## 12. Gestão da continuidade das atividades comerciais

A HP mantém de um programa global de continuidade de operações. Este programa adota uma abordagem holística, em toda a empresa, para a continuidade integral através de um conjunto de processos de planeamento colaborativos, normalizados e documentados internamente.

A HP exercita periodicamente os seus planos de continuidade das atividades profissionais para garantir a sua eficácia. Atualmente, a HP testa e atualiza todos os planos pelo menos uma vez por ano e assegura que as pessoas com funções no plano de continuidade das atividades comerciais recebem formação.

| Data de Revisão | Breve descrição da alteração | Autoridade de Revisão VC |
|---|---|---|
| Maio de 2018 | Publicação Inicial | Raella Dyke |
| Fevereiro de 2022 | Atualização | Grettel Acuña |