RIEPILOGO DELLE MISURE DI SICUREZZA

Al fine di proteggere i dati dei Clienti, HP applica una serie di rigorosi controlli delle informazioni, che includono politiche, pratiche, procedure e strutture organizzative, per salvaguardare la riservatezza, l'integrità e la disponibilità dei propri dati e di quelli dei suoi clienti, inclusi i Dati Personali, secondo la definizione degli Addendum di HP relativi ai Clienti e al Trattamento dei Dati. Di seguito viene fornita una panoramica delle misure tecniche e organizzative adottate da HP in tutta l'azienda.

1. Politica di sicurezza

HP gestisce politiche, standard e procedure, applicabili a livello globale, con lo scopo di proteggere i dati di HP e quelli dei Clienti. I dettagli delle politiche di sicurezza di HP vengono mantenuti riservati al fine di proteggere l'integrità dei dati e dei sistemi di HP. Di seguito viene tuttavia fornita una sintesi delle politiche principali.

2. Organizzazione per la sicurezza delle informazioni

HP ha un'Organizzazione per la sicurezza delle informazioni, responsabile di gestire e dirigere la sicurezza, la strategia e i controlli relativi alle informazioni dell'azienda. Sono stati istituiti un Sistema di Gestione e un Framework di Sicurezza delle Informazioni, allo scopo di garantire la conformità alle politiche e ai controlli di sicurezza di HP, oltre che di verificare il rispetto dei requisiti di sicurezza dei suoi clienti. Tale Framework è strutturato in linea con il Framework di sicurezza informatica del NIST e viene rivisto una volta l'anno.

3. Gestione degli asset

HP ha istituito un processo per l'identificazione degli asset di informazioni tecniche, che le permette di identificare tutti gli asset di cui è responsabile e di classificare quelli critici. HP utilizza anche una serie di procedure di gestione documentate per ogni categoria di informazioni, inclusi gli asset che contengono Dati Personali. Le procedure di gestione disciplinano archiviazione, trasmissione, comunicazione, accesso, registrazione, conservazione, distruzione, smaltimento, gestione degli incidenti e notifica delle violazioni.

4. Controllo degli accessi

Per garantire il controllo degli accessi viene utilizzato il principio del privilegio minimo. L'accesso utente viene garantito tramite una combinazione univoca di ID utente e password. Le politiche di HP in materia di password definiscono i controlli correlati alla complessità, all'efficacia, alla validità e alla cronologia delle password. I diritti di accesso vengono rivisti periodicamente e revocati alla cessazione del rapporto di lavoro.

Vengono implementate procedure di creazione ed eliminazione degli account reciprocamente

concordate per concedere e revocare l'accesso ai sistemi client utilizzati durante le interazioni.

5. Formazione del personale

I dipendenti HP devono completare il corso di formazione Integrità alla HP, che ha lo scopo di garantirne la familiarità con i programmi, le politiche e le risorse che disciplinano le aspettative di HP in materia di comportamento etico, eccellenza e conformità. Il corso Integrità alla HP include moduli dedicati alla sicurezza e alla riservatezza dei dati. I dipendenti sono inoltre tenuti a seguire un corso di aggiornamento annuale. I dipendenti HP devono completare anche un corso di aggiornamento annuale di sensibilizzazione alla sicurezza, incentrato sulle politiche di sicurezza essenziali, che sottolinea le responsabilità dei dipendenti in relazione alla gestione degli incidenti, alla riservatezza dei dati e alla sicurezza delle informazioni.

6. Terze parti e subappaltatori

HP ha istituito processi per la selezione di subappaltatori in grado di soddisfare tutti i requisiti di sicurezza contrattuali.

Per i fornitori applicabili (quelli che gestiscono, archiviano e trasmettono i dati di HP e i dati dei clienti in possesso di HP, o che hanno accesso alla rete HP), HP Cybersecurity effettua una valutazione dei rischi con lo scopo di verificare l'esistenza di un programma di sicurezza delle informazioni. Un programma adeguato deve includere misure di protezione fisiche, tecniche e amministrative. Tale valutazione deve essere eseguita prima di consentire ai fornitori di accedere alle informazioni di HP.

7. Sicurezza dei sistemi

In base alla politica aziendale, lo sviluppo dei sistemi e del software di supporto all'interno di HP segue una metodologia di sviluppo sicura, con lo scopo di garantire la protezione per l'intero ciclo di vita del software e dei sistemi. Il Ciclo di Sviluppo del Software definisce i requisiti di concezione, sviluppo/acquisizione, implementazione, funzionamento e smaltimento. Tutti i componenti dei sistemi, inclusi moduli, librerie, servizi e componenti discreti, vengono valutati al fine di determinarne l'impatto sul livello di sicurezza complessivo del sistema.

HP ha definito i controlli necessari per la protezione delle transazioni dei servizi applicativi. Tali controlli includono la convalida e la verifica delle credenziali utente, l'obbligo di crittografia e firma digitale, l'implementazione di protocolli di comunicazione sicuri e l'archiviazione dei dati delle transazioni online sui server all'interno della zona di sicurezza appropriata della rete.

Vengono regolarmente eseguite le scansioni delle vulnerabilità interne.

8. Sicurezza fisica e ambientale

Le strutture di HP sono protette da vari controlli di accesso fisici ed elettronici, oltre che da diversi sistemi di sorveglianza. A seconda della struttura, può trattarsi di guardie di sicurezza, controlli di accesso elettronici e televisori a circuito chiuso (CCTV, Closed-Circuit Television).

Tutto il personale di HP viene registrato ed è tenuto a indossare i badge identificativi appropriati.

Le strutture sono dotate del supporto appropriato per l'infrastruttura, con controlli di temperatura e alimentatori di riserva ove necessario, come UPS e/o generatori diesel, per garantire i servizi critici.

9. Gestione operativa

HP ha definito una serie di requisiti minimi per la protezione dell'infrastruttura tecnologica, che include workstation, server e apparecchiature di rete. Le immagini di workstation e server contengono sistemi operativi con protezione preventiva avanzata. I requisiti di protezione dipendono dal tipo di sistema operativo e dai controlli applicabili implementati.

HP ha implementato una serie di sistemi di prevenzione e rilevamento delle intrusioni (NIDS/NIPS, Network Intrusion Detection/Prevention System) nella rete, che vengono monitorati e gestiti 24 ore al giorno per 7 giorni la settimana.

Le politiche di sicurezza e gli standard HP impongono lo smaltimento sicuro dei supporti.

10. Crittografia

HP ha definito una serie di affidabili processi di crittografia con lo scopo di garantire la riservatezza, l'integrità e la disponibilità degli asset informativi. I protocolli approvati richiedono la crittografia di determinati asset, inclusi quelli che contengono Dati Personali.

11. Gestione degli incidenti di sicurezza delle informazioni

HP segue un avanzato Processo di Gestione degli Incidenti Informatici che copre finalità, ambito, ruoli, responsabilità, impegno di gestione, coordinamento dell'organizzazione, procedure di implementazione e controlli di conformità. HP rivede e aggiorna tale processo una volta l'anno.

Il Team di Risposta agli Incidenti Informatici, che include personale di HP Cybersecurity specializzato nella risposta agli incidenti e nella gestione delle situazioni di crisi, si riunisce regolarmente per la revisione teorica dei processi e degli eventuali incidenti o eventi.

12. Gestione della continuità operativa

HP segue un programma di Continuità Operativa, che adotta un approccio olistico esteso all'intera azienda, al fine di garantire la continuità end-to-end tramite una serie di processi di pianificazione collaborativi, standardizzati e documentati internamente.

HP effettua esercitazioni periodiche sui piani di continuità operativa allo scopo di garantirne l'efficacia. Attualmente HP verifica e aggiorna tutti i piani almeno una volta l'anno e garantisce la formazione di tutte le persone che ricoprono un ruolo specifico nel piano di continuità operativa.

Data revisione	Breve descrizione della modifica	POC autorità di revisione
Maggio 2018	Pubblicazione iniziale	Raella Dyke
Febbraio 2022	Aggiornamento	Grettel Acuña