Misure di Sicurezza

Presentato da:	**ADP - Global Security Organization**
Versione:	**2.0**
Data di rilascio:	**Settembre 2019**

Indice

Policy di Information Security	4
Organizzazione dell' Information Security	6
Sicurezza Risorse Umane	7
Gestione degli Asset	8
Controllo degli Accessi	9
Crittografia	10
Sicurezza Fisica ed Ambientale	11
Sicurezza Operativa	12
Sicurezza delle Comunicazioni	14
Nuovi Sistemi, Sviluppo e Manutenzione	15
Gestione dei Fornitori	16
Gestione degli Incidenti di Sicurezza	17
Aspetti di sicurezza delle informazioni della gestione della Resilienza del Business	18
Compliance	19

Termini e definizioni

I termini seguenti possono comparire in tutto il documento:

Termini o Acronimi utilizzati	Definizione
GETS	**Global Enterprise Technology & Solutions**
GSO	**Global Security Organization**
CAB	**Change Advisory Board**
DRP	**Disaster Recovery Plan**
CIRC	**GSO's Critical Incident Response Center**
SIEM	**Security Information and Event Management**
IDS	**Intrusion Detection System**
DNS	**Domain Name System**
NTP	**Network Time Protocol**
SOC	**Service Organization Controls**
TPSI	**Trusted Platform Security Infrastructure**

Overview

ADP mantiene un formale programma sulla sicurezza delle informazioni contenente garanzie amministrative, tecniche e fisiche per proteggere la sicurezza, la riservatezza e l'integrità delle informazioni dei clienti. Questo programma è ragionevolmente progettato per (i) salvaguardare la sicurezza e la riservatezza delle informazioni dei clienti, (ii) proteggere da minacce o rischi previsti per la sicurezza o l'integrità delle informazioni e (iii) proteggere dall' accesso non autorizzato o dall'uso delle informazioni .

Questo documento contiene una panoramica delle misure e delle pratiche della sicurezza delle informazioni di ADP, alla data di rilascio del documento e che sono soggette a modifiche da parte di ADP. Questi requisiti e pratiche sono progettati per essere coerenti con gli standard di sicurezza delle informazioni ISO / IEC 27001: 2013. ADP valuta periodicamente le proprie Policy e gli standard di sicurezza. Il nostro obiettivo è contribuire a garantire che il programma di sicurezza funzioni in modo efficace ed efficiente per proteggere tutte le informazioni a noi affidate dai nostri clienti e dai loro dipendenti.

Autonomia delle Funzioni di Information Security

Il reponsabile della Sicurezza di ADP (Chief Security Officer) è responsabile della struttura Global Security Organization (GSO) e riporta al General Counsel (Legal e Compliance), invece che al Chief Information Officer; ciò conferisce a GSO la necessaria indipendenza dall'IT. GSO è un team di sicurezza trasversale e divisionale che ha un approccio multidisciplinare in materia di sicurezza informatica, gestione dei rischi operativi, gestione della sicurezza dei clienti, protezione dei dipendenti ADP e della resilienza aziendale. Il senior management di GSO, a riporto del Chief Security Officer, è responsabile della gestione delle Policy, delle procedure e delle linee guida di sicurezza.

Definizione Formale delle Policy di Information Security

ADP ha sviluppato e documentato le policy di Information Security che definiscono l'approccio di ADP alla gestione della sicurezza delle informazioni. Le aree specifiche coperte da queste policy includono, ma non sono limitate a:

- **Security Management Policy** – Definisce le responsabilità della Global Security Organization (GSO) e del Chief Security Officer (CSO), comprese le responsabilità sulla sicurezza delle informazioni e i controlli sul processo di assunzione dal punto di vista della sicurezza.
- **Global Privacy Policy –** Relativa alla raccolta di informazioni personali, l'accesso, l'accuratezza, la divulgazione e l'informativa sulla privacy ai clienti.
- **Utilizzo consentito da parte dei dipendenti delle comunicazioni elettroniche e Policy sulla protezione dei dati** – Descrive l'uso accettabile delle diverse comunicazioni elettroniche, la crittografia e la gestione delle chiavi.
- **Policy sulla gestione delle informazioni –** Fornisce requisiti per la classificazione delle informazioni ADP e stabilisce i controlli di protezione.
- **Policy sulla Sicurezza Fisica –** Definisce i requisiti di sicurezza delle strutture ADP per i visitatori e per i nostri dipendenti che vi lavorano.
- **Policy della gestione della Sicurezza Operativa –** Fornisce controlli minimi per la manutenzione delle patch di sistema, proteggersi efficacemente dalla minaccia dei malware, gestione dei backup e controlli di sicurezza dei database.
- **Policy sul Monitoraggio della Sicurezza –** Fornisce controlli per sistemi di rilevamento delle intrusioni (IDS), log e prevenzione della perdita di dati (DLP).
- **Policy sulle Investigazioni e gestione degli Incidenti –** Definisce gli standard per la risposta agli incidenti, le indagini forensi, la protezione della forza lavoro e l'accesso alle informazioni elettroniche archiviate dei dipendenti.
- **Policy di Accesso & Autenticazione –** Descrive i requisiti di autenticazione (ad es. ID utente e password), accesso remoto e accesso alle reti wireless.
- **Policy sulla Sicurezza della Rete –** Definisce l'architettura di sicurezza di router, firewall, AD, DNS, server di posta elettronica, DMZ, servizi cloud, dispositivi di rete, proxy Web e tecnologia di rete commutata.
- **Policy Globale sulle Terze Parti e Acquisizioni –** Definisce controlli minimi di sicurezza per coinvolgere terze parti per aiutare ADP a raggiungere i propri obiettivi aziendali.
- **Policy sulla Gestione delle Applicazioni –** Stabilisce adeguati controlli di sicurezza in ogni fase del ciclo di vita dello sviluppo del sistema.
- **Policy sulla Business Resiliency –** Gestisce la protezione, l'integrità e la conservazione del Business di ADP stabilendo i requisiti minimi per documentare, implementare, mantenere e migliorare continuamente i programmi di resilienza aziendale.

- **Policy sulla Converged Security Risk Management–** Identificazione, monitoraggio, risposta, analisi, governance e nuove iniziative commerciali.

Le Policy sono pubblicate nella Intranet ADP e sono accessibili a tutti gli associate e i fornitori, all'interno della rete ADP.

Revisione delle Policy di Information Security

ADP rivede le sue Policy di sicurezza delle informazioni almeno una volta all'anno o ogni volta che ci sono cambiamenti importanti che incidono sul funzionamento dei sistemi di informazione di ADP.

Organizzazione dell' Information Security

Ruoli e Responsabilità dell'Information Security

Il GSO è costituito da diversi team di sicurezza strutturati che adottano un approccio multidisciplinare al rispetto degli standard di sicurezzainformatica, gestione dei rischi operativi, gestione della sicurezza dei clienti, protezione della forza lavoro e resilienza aziendale. I ruoli e le responsabilità sono stati definiti formalmente per tutti i membri del Team. Il GSO è incaricato della progettazione, dell'implementazione e della supervisione del nostro programma di sicurezza delle informazioni basato sulle Policy aziendali. Le attività di GSO sono supervisionate dall'Executive Security Committee, i cui membri includono Chief Security Officer, Chief Executive Officer, Chief Financial Officer, Chief Strategy Officer, Chief Human Resources Officer e il General Counsel di ADP.

Mobile Computing and Teleworking Policy

ADP richiede che tutte le informazioni riservate siano crittografate sui dispositivi mobili, per prevenire la perdita di dati, che potrebbe derivare dal furto o dalla perdita di un computer / dispositivo. Per accedere alle reti aziendali da remoto sono inoltre necessarie la protezione avanzata degli endpoint e l'autenticazione a due fattori tramite VPN. Tutti i dispositivi remoti devono essere protetti da password. I dipendenti ADP sono tenuti a segnalare immediatamente i dispositivi persi o rubati attraverso un processo di segnalazione di incidenti di sicurezza.

Tutti i dipendenti e i fornitori, come condizione per l'impiego presso ADP, devono rispettare la Policy sull'uso accettabile delle comunicazioni elettroniche e della protezione dei dati e altre Policy pertinenti.

Background Checks

Coerentemente con i requisiti legali applicabili nella giurisdizione della persona, ADP effettua adeguati controlli di base commisurati ai doveri e alle responsabilità dei suoi dipendenti, appaltatori e terze parti. Questi controlli confermano l'idoneità del candidato a gestire le informazioni dei clienti prima di ingaggiare o assumere tali soggetti.

I controlli possono includere includere i seguenti componenti:

- Verifica dell'ammissibilità identità / impiego.
- Storico lavorativo precedent impieghi.
- Curriculum scolastico e qualifiche professionali
- Casellario giudiziale (ove legalmente autorizzato e in base alle normative locali)

Accordi di riservatezza con dipendenti e appaltatori

I contratti di lavoro e i contratti con gli appaltatori contengono termini che indicano gli obblighi e le responsabilità relative alle informazioni sui clienti a cui avranno accesso. Tutti i dipendenti e gli appaltatori di ADP sono vincolati da obblighi di riservatezza.

Programmi di Formazione sulla Sicurezza delle Informazioni

Tutti i dipendenti sono tenuti a completare la formazione sulla sicurezza delle informazioni come parte del loro piano di inserimento in azienda. Inoltre, ADP offre una formazione annuale sulla sicurezza per ricordare ai dipendenti le loro responsabilità quando svolgono le loro attività quotidiane..

Responsabilità degli associate e Processi Disciplinari

ADP ha pubblicato delle Policy di sicurezza che tutti i dipendenti ADP devono rispettare. Le violazioni delle Policy di sicurezza possono comportare la revoca dei privilegi di accesso e / o azioni disciplinari fino alla risoluzione dei contratti di consulenza o dell'impiego.

Cessazione delle responsabilità lavorative

Le responsabilità in caso di cessazione del rapporto di lavoro sono state formalmente documentate e comprendono :

- Restituire tutte le informazioni e le risorse ADP in possesso del rispettivo dipendente, su qualsiasi supporto sia memorizzato.
- Cessazione dei diritti di accesso a strutture, informazioni e sistemi ADP
- Modifica delle password per gli account condivisi attivi rimanenti, se applicabile
- Passaggio di consegne, se applicabile.

Gestione degli Asset

Utilizzo consentito dei dispositivi

L'uso accettabile delle risorse è spiegato in diverse Policy, applicabili a dipendenti e fornitori di ADP, per aiutare a garantire che le informazioni di ADP e dei clienti non siano esposte dall'uso di tali risorse. Esempi di aree descritte in queste Policy sono: l'uso di comunicazioni elettroniche, l'uso di apparecchiature elettroniche e l'uso di risorse informatiche.

Classificazione delle Informazioni

Le informazioni acquisite, create o gestite da o per conto di ADP ricevono, a seconda dei casi, una classificazione di sicurezza di:

- Public - Esempio: opuscoli di marketing, relazioni annuali pubblicate.
- ADP Internal Use Only - Esempio: comunicazioni tra uffici, procedure operative.
- ADP Confidential - Esempio: informazioni personali personali e sensibili.
- ADP Restricted - Esempio: previsioni finanziarie, informazioni sulla pianificazione strategica.

I requisiti per la gestione delle informazioni sono direttamente correlati alla classificazione della sicurezza delle informazioni. Le informazioni personali e le informazioni personali sensibili sono sempre considerate ADP Confidential. Tutte le informazioni del cliente sono classificate come riservate.

I dipendenti ADP sono responsabili della protezione e della gestione delle informazioni in conformità con il loro livello di classificazione di sicurezza, che fornisce il grado di protezione delle informazioni e requisiti di gestione applicabili per ciascun livello di classificazione. La classificazione di riservatezza ADP viene applicata a tutte le informazioni archiviate, trasmesse o gestite da terzi.

Smaltimento di Apparecchiature e Supporti

Quando apparecchiature, documenti, file e supporti di ADP vengono eliminati o riutilizzati, vengono prese le misure appropriate per impedire il successivo recupero delle informazioni del cliente originariamente memorizzate in essi. Tutte le informazioni su computer o supporti di archiviazione elettronici, indipendentemente dalla classificazione, vengono eliminate in modo sicuro, a meno che il supporto non venga distrutto fisicamente, prima di essere rilasciato al di fuori delle strutture ADP o riutilizzato. Le procedure per la distruzione / cancellazione sicura delle informazioni ADP contenute nelle apparecchiature, in documenti, file e supporti sono formalmente documentate.

Supporti fisici in transito

Sono state implementate misure organizzative per proteggere i materiali stampati contenenti le informazioni dei clienti contro furto, perdita e / o accesso / modifica non autorizzati (i) durante il transito, ad es. buste sigillate, contenitori e consegna a mano all'utente autorizzato; e (ii) durante la revisione, o altri trattamenti se rimossi dall'archiviazione sicura.

Controllo degli Accessi

Requisiti del Business sul Controllo Accessi

La Policy di controllo degli accessi di ADP si basa su requisiti definiti dall'azienda. Le Policy e gli standard di controllo sono articolati in controlli di accesso che vengono applicati in tutti i componenti del servizio fornito e si basano su un principio di "privilegio minimo" e "necessità di conoscere".

Accesso alle infrastrutture - Gestione del controllo degli accessi

Le richieste di accesso per lo spostamento, l'aggiunta, la creazione e l'eliminazione vengono registrate, approvate e riviste periodicamente.

Una revisione formale viene eseguita, almeno una volta all'anno, per confermare che i singoli utenti corrispondano esattamente al ruolo aziendale rilevante e che non avrebbero continuato l'accesso dopo un cambio di posizione. Questo processo è verificato e documentato in un rapporto SOC1[1] di tipo II. Dall'interno di un sistema di gestione dell'identità, un team ADP dedicato è responsabile della concessione, della negazione, dell'annullamento, della conclusione e della disattivazione / disattivazione dell'accesso alle strutture e ai sistemi di informazione ADP. ADP utilizza uno strumento di gestione centralizzata delle identità e degli accessi (IAM) gestito centralmente da un team GETS dedicato. In base ai diritti di accesso richiesti tramite lo strumento IAM centralizzato, verrà attivato un flusso di lavoro di convalida che potrebbe coinvolgere il supervisore degli utenti. L'accesso è fornito su base temporanea ed esistono flussi di lavoro per impedire che tale accesso rimanga permanente. L'accesso di un dipendente a una struttura viene disattivato immediatamente dopo l'ultimo giorno di assunzione disattivando la sua carta di accesso (badge del dipendente). Gli ID utente del dipendente vengono immediatamente disattivati. Tutte le risorse dei dipendenti vengono restituite e controllate dal responsabile di linea competente e confrontate con l'elenco delle risorse nella base dati di gestione della configurazione. A seguito di una modifica della posizione lavorativa o di modifiche organizzative, i profili utente o i diritti di accesso degli utenti devono essere modificati dalla direzione della business unit e dal team IAM. Inoltre, ogni anno viene eseguita una revisione formale dei diritti di accesso per verificare che i diritti dei singoli utenti corrispondano al loro ruolo commerciale rilevante e che non vi siano diritti di accesso irrilevanti rimanenti dopo un trasferimento di posizione.

Password Policy

I criteri password associati ADP vengono applicati ai server, database, dispositivi e applicazioni di rete, nella misura consentita dal dispositivo / applicazione. La complessità della password deriva da un'analisi basata sul rischio dei dati e dei contenuti protetti. Le Policy soddisfano gli standard di settore prevalenti in termini di robustezza e complessità, incluso ma non limitato all'uso dell'autenticazione step-up, a due fattori o biometrica laddove appropriato.

I requisiti di autenticazione delle applicazioni client variano in base al prodotto e i servizi federati (SAML 2.0) sono disponibili su applicazioni ADP specifiche utilizzando una rete unificata e un livello di sicurezza gestito da GETS.

Timeout delle Sessioni

ADP applica timeout automatici a tutti i server, workstation, applicazioni e connessioni VPN basati su un approccio basato sul rischio coerente con gli standard del settore. Il ripristino delle sessioni può avvenire solo dopo che l'utente ha fornito una password valida.

[1] Nel caso di alcuni servizi statunitensi offerti da ADP, è disponibile anche un report SOC 2 Type II.

Crittografia

Controlli Crittografici

ADP richiede che le informazioni sensibili scambiate tra ADP e terze parti ADP debbano essere crittografate (o che il canale di trasporto debba essere cifrato) utilizzando tecniche di crittografia accettati dagli Standard del settore. In alternativa, è possibile utilizzare una linea dedicata.

Gestione delle Chiavi di Cifratura

ADP ha uno standard interno di sicurezza della crittografia che include una gestione delle chiavi ben definita e procedure di deposito delle chiavi, compresa la gestione delle chiavi sia simmetrica che asimmetrica.

Le chiavi di crittografia utilizzate per le informazioni ADP sono sempre classificate come informazioni riservate. L'accesso a tali chiavi è strettamente limitato a coloro che hanno bisogno di sapere e, se viene fornita un'approvazione alle eccezioni. Le chiavi di crittografia e la gestione del ciclo di vita delle chiavi hanno seguito le pratiche standard del settore.

Sicurezza Fisica ed Ambientale

L'approccio di ADP alla sicurezza fisica ha due obiettivi: creare un ambiente di lavoro sicuro per i dipendenti ADP e proteggere le informazioni personali conservate nei data center ADP e in altri uffici strategici di ADP.

La Policy di sicurezza ADP richiede che la gestione ADP identifichi quelle aree che richiedono un livello specifico di sicurezza fisica. L'accesso a tali aree è fornito solo agli associati autorizzati per scopi autorizzati. Le aree protette dell'ADP adottano varie garanzie di sicurezza fisica, inclusi i sistemi di videosorveglianza, l'uso dei badge di sicurezza (accesso controllato dalle identità) e le guardie di sicurezza di stanza ai punti di entrata e di uscita. Ai visitatori può essere concesso l'accesso solo se autorizzati e sono accompagnati in ogni momento.

Sicurezza Operativa

Formalizzazione delle procedure operative IT

GETS è l'unità ADP responsabile delle operazioni e della manutenzione dell'infrastruttura IT. GETS mantiene e documenta formalmente le Policy e le procedure relative alle operazioni IT. Queste procedure includono, ma non sono limitate a quanto segue:

- Gestione degli aggiornamenti.
- Gestione del backup
- Gestione degli errori di sistema
- Riavvio e ripristino del sistema
- Monitoraggio del sistema
- Pianificazione e monitoraggio dei lavori

Gestione degli Aggiornamenti dell'Infrastruttura

Il Change Advisory Board (CAB), che comprende rappresentanti di una vasta gamma di Team ADP, è coordinato da GETS. Le riunioni CAB discutono dell'impatto, le finestre di distribuzione dei rilasci in produzione, nonché per coordinare qualsiasi altro cambiamento nell'infrastruttura di produzione.

Pianificazione dell'Approvigionamento dei Sistemi

I requisiti di capacità sono costantemente monitorati e rivisti periodicamente. A seguito di queste revisioni, i sistemi e le reti vengono dimensionati di conseguenza. Quando devono essere apportate modifiche significative a causa di una modifica della capacità o di un'evoluzione tecnologica, il team di benchmarking GETS può eseguire prove di stress per l'applicazione e / o il sistema pertinenti. Al termine delle prove di stress, il team fornisce un rapporto dettagliato sull'evoluzione delle prestazioni misurando le modifiche in (i) componenti, (ii) configurazione o versione del sistema o (iii) configurazione o versione del middleware.

Protezione contro Codice Malevolo

Le tecnologie di protezione degli endpoint vengono implementate per proteggere le risorse ADP in conformità con i migliori standard del settore.

Policy sulla Gestione dei Backup

ADP ha messo in atto delle Policy che richiedono che tutte le operazioni di hosting di produzione eseguano il backup delle informazioni. L'ambito e la frequenza dei backup vengono eseguiti in conformità con i requisiti aziendali dei servizi ADP pertinenti, i requisiti di sicurezza delle informazioni interessate e la criticità delle informazioni in relazione al ripristino di emergenza. Il monitoraggio dei backup pianificati viene eseguito da GETS per identificare problemi di backup o eventuali eccezioni.

Sicurezza dei Log e Monitoraggio

ADP ha implementato un'infrastruttura di registrazione centrale e di sola lettura (SIEM) e un sistema di correlazione dei log e avvisi di allarme (TPSI). Gli avvisi provenienti dai log sono monitorati e trattati in modo tempestivo dal CIRC.

Tutti questi sistemi sono sincronizzati utilizzando un unico riferimento basato su Network Time Protocol (NTP).

Ogni singolo log deve contenere almeno:

- Data e Ora
- Chi (identificazione dell'operatore o amministratore)
- Cosa (Informazioni sull'evento)

Gli audit trail e la registrazione del sistema per le applicazioni ADP sono progettati e configurati per tenere traccia delle seguenti informazioni:

- Accesso autorizzato
- Operazioni privilegiate
- Tentativi di accesso non autorizzati
- Avvisi o guasti dei sistemi
- Modifiche alle impostazioni di sicurezza del sistema, quando il sistema consente tale registrazione

Questi registri sono disponibili solo per il personale autorizzato ADP e vengono inviati in modalità live per impedire che i dati vengano manomessi prima di essere archiviati nelle apparecchiature di registrazione sicure.

Monitoraggio Systemi IT

ADP utilizza misure appropriate per il monitoraggio dell'infrastruttura 24 ore al giorno, 7 giorni alla settimana. Gli avvisi di sono gestiti da diversi team in base al livello di gravità e alle competenze necessarie per risolverli.

Le strutture del centro di hosting ADP utilizzano applicazioni di monitoraggio costantemente in esecuzione su tutti i sistemi di elaborazione correlati e sui componenti di rete per fornire allo staff ADP una notifica proattiva di problemi e avvisi in previsione di possibili problemi.

Gestione Tecnica delle Vulnerabilità

Tutti i server installati nell'infrastruttura di hosting devono essere conformi ai criteri per l'installazione di un sistema operativo sicuro (o processo di Hardening). Le operazioni ospitate utilizzano una versione approvata e standardizzata per ogni tipo di server utilizzato all'interno della nostra infrastruttura. L'installazione immediata di sistemi operativi è vietata poiché queste installazioni possono creare vulnerabilità, come password generiche di account di sistema, che potrebbero comportare rischi per l'infrastruttura. Queste configurazioni riducono l'esposizione dei computer che eseguono servizi non necessari che possono causare vulnerabilità.

ADP adotta una metodologia documentata per condurre rilasci e valutazioni periodiche delle vulnerabilità ,revisioni della conformità delle applicazioni basate su Internet e dei relativi componenti dell'infrastruttura, che includono almeno 15 categorie primarie di test. La metodologia di valutazione si basa sulle migliori pratiche interne e di settore, inclusi, a titolo esemplificativo, Open Web Application Security Project (OWASP), SANS Institute e Web Application Security Consortium (WASC)

Sicurezza delle Comunicazioni

Gestione della Sicurezza della Rete

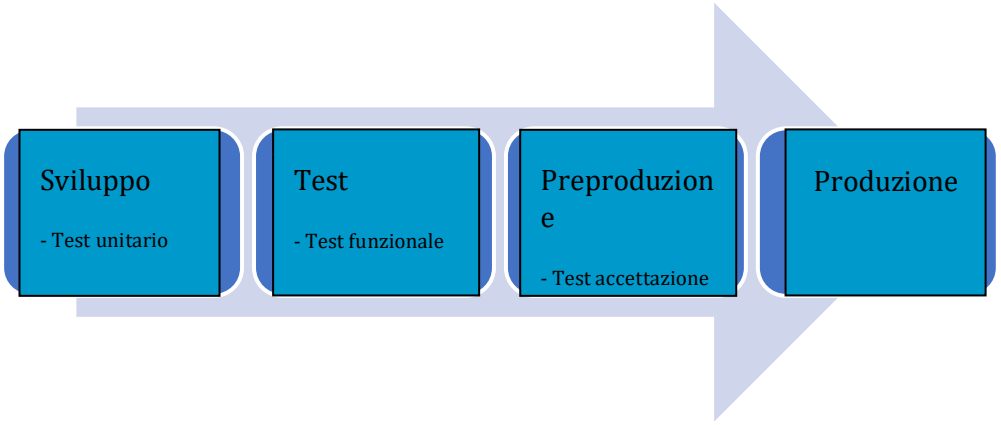
ADP utilizza un sistema di rilevamento delle intrusioni basato sulla rete che monitora il traffico a livello di infrastruttura di rete (24 ore al giorno, 7 giorni alla settimana) e identifica attività sospette o potenziali attacchi.

Scambio di Informazioni

ADP implementa controlli adeguati in modo che le informazioni dei clienti ADP inviate a terzi vengano trasferite solo tra i sistemi e le risorse di informazioni autorizzate e vengano scambiate solo attraverso i meccanismi di trasferimento sicuri e autorizzati di ADP.

Gestione dello Sviluppo e dei Processi di Supporto

Durante il ciclo di sviluppo, viene generata la documentazione applicabile e vengono creati piani di test per la fase di test. Sono definite diverse fasi per ciascun ambiente con l'approvazione pertinente in ciascuna fase:



- Per passare dall'ambiente di test all'ambiente di pre-produzione, è necessaria l'approvazione del team di qualità di ADP.
- Per passare dalla pre-produzione alla produzione, è necessaria l'approvazione delle operazioni IT.

I team di sviluppo sono tenuti ad utilizzare metodi di codifica sicuri. Le modifiche alle applicazioni vengono testate negli ambienti di sviluppo e regressione prima che raggiungano i sistemi di produzione. I test vengono eseguiti e documentati. Dopo l'approvazione, le modifiche vengono implementate nella produzione. Il test di penetrazione viene eseguito dopo cambiamenti significativi.

Un CAB periodico, che include rappresentanti di una vasta gamma di team ADP, è tenuto da GETS. Le riunioni CAB si svolgono su base regolare e hanno lo scopo di discutere gli impatti, concordare finestre di distribuzione e approvare la promozione di pacchetti software per la produzione, nonché per informare su eventuali altri cambiamenti nell'infrastruttura di produzione.

Il team operativo IT di ADP fornisce l'approvazione finale prima della promozione nell'ambiente di produzione dei pacchetti software.

Sicurezza negli Ambienti di Produzione

Gli ambienti di produzione e sviluppo sono separati e indipendenti l'uno dall'altro. Controlli di accesso adeguati sono impiegati per imporre una corretta separazione delle funzioni. I pacchetti software sono accessibili in ogni fase del processo di sviluppo e solo dai team coinvolti in quella fase.

Dati di Test

Secondo la Policy di gestione delle applicazioni di ADP, l'uso di dati reali o non anonimizzati in sviluppo e test non è consentito se non esplicitamente richiesto e autorizzato dal cliente.

Gestione dei Fornitori

Identificazione dei rischi relativi a terze parti esterne

Le valutazioni dei rischi di terzi che richiedono l'accesso ad ADP e / o informazioni sui clienti vengono periodicamente eseguite per determinare la loro conformità ai requisiti di sicurezza di ADP per i terzi e per identificare eventuali lacune nei controlli applicati. Se viene identificato un gap di sicurezza, vengono concordati nuovi controlli con tali soggetti esterni.

Accordi di sicurezza delle informazioni con parti esterne

ADP stipula accordi con tutte le terze parti che includono impegni di sicurezza adeguati per soddisfare i requisiti di sicurezza di ADP.

Gestione degli Incidenti di Sicurezza

Gestione degli incidenti e dei miglioramenti della sicurezza delle informazioni

ADP ha una metodologia documentata per rispondere agli incidenti di sicurezza in modo tempestivo, coerente ed efficace.

In caso di incidente, un team predefinito di dipendenti ADP attiva un piano formale di risposta agli incidenti che affronta aree come:

- Escalation basate sulla classificazione della gravità dell'incidente
- Elenco contatti per la segnalazione / escalation di incidenti
- Linee guida per le risposte iniziali e follow-up con i clienti coinvolti
- Conformità alle leggi di notifica delle violazioni della sicurezza applicabili
- Registro delle indagini
- Ripristino del sistema
- Risoluzione dei problemi, rapporti e revisione
- Causa principale e rimedi
- Lesson Learned

Le Policy ADP definiscono un incidente di sicurezza, la gestione degli incidenti e tutte le responsabilità dei dipendenti in merito alla segnalazione di incidenti di sicurezza. ADP organizza regolarmente corsi di formazione per dipendenti e appaltatori di ADP per contribuire a garantire la consapevolezza dei requisiti di segnalazione. La formazione viene tracciata per garantire il completamento.

Aspetti di sicurezza delle informazioni della gestione della Resilienza del Business

ADP Business Resiliency Program

ADP è impegnata a mantenere i nostri servizi e le nostre operazioni in modo regolare, in modo da poter fornire ai nostri clienti il miglior servizio possibile. È la nostra priorità identificare - e mitigare - i rischi tecnologici, ambientali, di processo e sanitari che potrebbero ostacolare la fornitura dei nostri servizi aziendali. ADP ha creato un framework integrato che definisce i nostri processi di mitigazione, preparazione, risposta e recupero e include:

- Valutazione del rischio
- Analisi delle minacce al rischio
- Analisi dell'impatto sul business
- Pianificare lo sviluppo
- Pianificazione della continuità operativa
- Pianificazione del ripristino di emergenza
- Pianificazione della salute e della sicurezza
- Risposta nel mondo reale
- Gestione della crisi
- Risposta di emergenza
- Test e convalida
- Revisione
- Esercizio

Compliance

Compliance con le Policy di Sicurezza e gli Standard

ADP utilizza un processo per eseguire internamente revisioni della conformità su base periodica. Inoltre, ADP esegue un audit di tipo SOC1[2] tipo II su base periodica. Tali audit sono condotti da una nota società di revisione di terze parti e i rapporti di audit sono disponibili su base annuale per i clienti su richiesta, ove applicabile.

Compliance Tecnica

Per far rispettare la conformità tecnica con le migliori pratiche, ADP esegue scansioni di vulnerabilità della rete regolarmente pianificate. I risultati della scansione vengono quindi definiti in ordine di priorità e sviluppati in piani di azioni correttive con i team di hosting e la loro gestione.

Le scansioni delle vulnerabilità vengono eseguite su base regolare sia in ambienti interni che esterni. Inoltre, le scansioni del codice sorgente e i test di penetrazione vengono eseguiti in base al prodotto. Utilizzando strumenti specializzati di scansione delle applicazioni, le eventuali vulnerabilità a livello di applicazione vengono identificate, condivise con i team di gestione dello sviluppo del prodotto e incorporate nei processi di garanzia della qualità per azioni correttive. I risultati vengono analizzati e piani d'azione correttivi sviluppati e prioritari.

Retention dei Dati

La Policy di conservazione dei dati di ADP relativa alle informazioni sui clienti è progettata per conformarsi alle leggi applicabili. Alla fine di un contratto cliente, ADP rispetta i propri obblighi contrattuali relativi alle informazioni del cliente. ADP restituirà o consentirà al client di recuperare (mediante download di dati), tutte le informazioni del cliente richieste per la continuità delle attività commerciali del cliente (se non fornite in precedenza). Quindi, ADP distruggerà in modo sicuro le informazioni rimanenti sul cliente, tranne nella misura richiesta dalla legge applicabile, autorizzata dal cliente o necessaria ai fini della risoluzione delle controversie.

[2] Nel caso di alcuni servizi statunitensi offerti da ADP, è disponibile anche un report SOC 2 Type II.