Piano di Assicurazione Sicurezza

Infomaniak Network

Indice

1. Cronologia

Data	Autore	Funzione	Natura della modifica
13.05.2025	Johann Laqua	RSSI	Modifica del logo aziendale, aggiornamento dei capitoli sulla sicurezza fisica, aggiunta del capitolo sulle definizioni
19.04.2024	Johann Laqua	RSSI	Finalizzazione del documento per la prima pubblicazione
14.02.2024	Johann Laqua	RSSI	Prima versione del documento

2. Informazioni sul presente documento

Lo scopo di questo documento è presentare il Piano di Assicurazione Sicurezza di Infomaniak Network SA.

3. Introduzione

3.1. Oggetto del documento

Il presente documento stabilisce il nostro Piano di Assicurazione Sicurezza (PAS) che può essere allegato ai contratti con i nostri clienti. Il presente piano definisce gli impegni assunti da Infomaniak Network per soddisfare i requisiti contrattuali in materia di Sicurezza dei Sistemi Informativi (SSI). Questi ultimi hanno lo scopo di:

- garantire la protezione delle risorse dei sistemi informativi utilizzati nella prestazione di servizi convenuti contrattualmente;
- proteggere i nostri clienti da qualsiasi danno che possa derivare dall'indisponibilità di tali risorse, nonché da qualsiasi violazione della loro integrità o riservatezza.

Il nostro Piano di Assicurazione Sicurezza (PAS) illustra in dettaglio le varie disposizioni relative alla sicurezza, incluse le misure fisiche, organizzative, procedurali e tecniche che abbiamo implementato.

3.2. Campo di applicazione

Il presente documento riguarda i servizi gestiti dai team di Infomaniak Network e le loro attività.

3.3. Evoluzione

Qualsiasi modifica apportata al Piano di Assicurazione Sicurezza (PAS) comporta una nuova versione del presente documento. Le modifiche apportate vengono inserite e datate nella cronologia delle versioni incluse nel documento.

Il Piano di Assicurazione Sicurezza (PAS) viene esaminato almeno una volta all'anno dai responsabili della conformità e della sicurezza dei sistemi informativi e quindi approvato dalla direzione.

3.4. Definizioni

RSSI: Responsabile della sicurezza dei sistemi informatici
ISO: Organizzazione internazionale di normazione
EBIOS: Espressione dei bisogni e individuazione degli obiettivi di sicurezza
Red team: Team addetto alla sicurezza incentrato sullo svolgimento di esercitazioni e test di sicurezza offensiva, costituito da persone provenienti da diversi reparti.
ASDPO: Associazione svizzera dei delegati alla protezione dei dati
NCSC: National cyber security centre
CERT: Computer emergency response team
RH: Risorse umane
HTTPS: Hypertext transfer protocol secure

SSL: Secure sockets layer
IMAPS: Internet message access protocol secure
SMTPS: Simple mail transfer protocol secure
POP3S: Post office protocol 3 secure
IDS: Intrusion detection system
DDoS: Distributed denial of service
CVE: Common vulnerabilities and exposures
PCA: Piano di continuità operativa
RPO: Recovery point objective
RTO: Recovery time objective
LPD: Legge federale sulla protezione dei dati
RGPD: Regolamento generale sulla protezione dei dati

4. Buone pratiche

La sicurezza di Infomaniak Network è gestita da un comitato di sicurezza, nonché da un team di conformità secondo gli standard ISO 27001 per l'intera impresa. Infomaniak Network è certificata ISO 27001:2022 sui perimetri e sulle attività seguenti:

Sviluppo e fornitura di infrastrutture cloud, servizi web, applicazioni, assistenza clienti, manutenzione operativa dei data center.

5. Gestione dei rischi

Infomaniak Network ha formalizzato una valutazione scritta dei rischi che copre l'intero campo di applicazione del piano di assicurazione sicurezza, applicando una metodologia documentata in grado di garantire la riproducibilità e la comparabilità dell'approccio.

Il processo di valutazione dei rischi comprende un'analisi, una gestione e piani di mitigazione dei rischi che portano a misure e progetti concreti.

Infomaniak Network si affida inoltre a metodi ampiamente riconosciuti, quali EBIOS RM per gestire i rischi nel quadro del proprio sistema di gestione della sicurezza delle informazioni (SMSI).

6. Politica di sicurezza delle informazioni

Il documento sulla Politica di sicurezza di Infomaniak Network è disponibile a questo indirizzo: https://www.infomaniak.com/documents/politique_SI_EE_it.pdf

Il documento illustra chiaramente i nostri impegni e i nostri obiettivi in materia di sicurezza delle informazioni.

7. Organizzazione della sicurezza delle informazioni

Per strutturare il nostro approccio in materia di sicurezza dei sistemi informatici (SSI), abbiamo sviluppato diversi strumenti complementari: un organigramma specifico per l'SSI, una politica interna per la sicurezza dei sistemi informatici (PSSI) e un sistema di gestione della sicurezza delle informazioni (SMSI). Si tratta di elementi essenziali per garantire un'applicazione rigorosa e coerente delle nostre procedure di sicurezza.

7.1. Ruoli e responsabilità

Sono state definite e attribuite le responsabilità in materia di sicurezza.

Infomaniak Network ha nominato un Chief Information Security Officer (CISO). Questa persona supervisiona tutte le misure tecniche e organizzative implementate nel quadro della nostra strategia globale di sicurezza delle informazioni.

Un comitato di sicurezza, composto dai responsabili dei vari dipartimenti e team tecnici dell'azienda, si riunisce settimanalmente per riunioni SOC (Security Operations Center) per discutere argomenti relativi alla sicurezza delle informazioni.

Sotto la supervisione del CISO, un team Red Team effettua test di sicurezza sui prodotti e test di ingegneria sociale sui collaboratori dell'azienda.

7.2. Governance

È stato istituito un team dedicato alla governance a livello strategico e operativo.

Il team si riunisce regolarmente per supervisionare le questioni relative alla sicurezza dei sistemi informatici. I verbali delle riunioni vengono conservati in modo sicuro.

7.3. Rapporti con gli enti e le autorità

Infomaniak Network è membro di un'associazione di categoria (ASDPO) e intrattiene le relazioni con le autorità (NCSC e Cyber Security Hub) per gli sviluppi nel settore della sicurezza delle informazioni.

7.4. Sorveglianza e sicurezza

All'interno dell'attività è in atto un servizio di sorveglianza della sicurezza, tecnica e legale. Consente
di prevenire i rischi specificamente legati alle attività di Infomaniak Network.

Infomaniak Network si basa su una partnership con un'azienda specializzata in cybersicurezza per assicurare un monitoraggio sul dark web per gli asset sensibili sotto la propria responsabilità.

8. Sicurezza delle risorse umane

8.1. Reclutamento

Il nostro reparto HR applica una procedura di reclutamento per ogni candidato all'assunzione con misure di sicurezza proporzionali al livello di inquadramento di ogni addetto e ai rischi identificati.

Vengono effettuate le seguenti verifiche:

- Controllo dell'identità del candidato
- Verifica delle competenze della posizione
- Verifica delle referenze del candidato
- Verifica del casellario giudiziario
- Verifica approfondita dei precedenti per i candidati agli alti livelli di sicurezza

8.2. Gestione della riservatezza

I contratti di lavoro stabiliscono chiaramente le responsabilità del personale in materia di sicurezza delle informazioni.

Una clausola di riservatezza, estratta dalle condizioni generali del contratto di lavoro, impegna il personale a rispettare rigorosamente la riservatezza dei dati sensibili e privati ai quali ha accesso nell'ambito dello svolgimento delle sue funzioni presso Infomaniak. Qualsiasi violazione di questa clausola comporta conseguenze per il trasgressore.

Inoltre, è stato istituito un procedimento disciplinare formale a sua volta comunicato a tutti i membri del personale e alle altre parti interessate. Tale processo prevede sanzioni adeguate nei confronti di chiunque abbia violato le regole sulla sicurezza delle informazioni.

8.3. Sensibilizzazione alla sicurezza

Organizziamo sessioni di integrazione sulla sicurezza per verificare la conformità delle postazioni di lavoro e sensibilizzare i colleghi sui rischi legati alla sicurezza dei sistemi informatici (SSI) e alle nostre procedure di sicurezza fisica e logica.

Durante queste sessioni, presentiamo anche documenti importanti come la nostra Politica di Sicurezza delle Informazioni (PSI), nonché le nostre Linee Guida Generali sulla sicurezza.

Ogni anno elaboriamo un programma di sensibilizzazione utilizzando diversi strumenti di valutazione su vari temi legati alla sicurezza e alla cybersicurezza. Ciò include anche campagne di phishing e social engineering.

Diverse comunicazioni ai collaboratori vengono effettuate via e-mail allo scopo di sensibilizzarli sui rischi di sicurezza delle informazioni, sulla protezione dei dati, sui cyber-rischi nonché sugli aggiornamenti del nostro sistema di gestione della sicurezza delle informazioni.

8.4. Carta informatica

Infomaniak Network dispone di Linee Guida Generali sulla Sicurezza equivalenti a una carta informatica che vengono regolarmente aggiornate e comunicate a tutti i membri della nostra impresa.

Fin dalla loro assunzione e ogni anno si impegnano solennemente a rispettarli, pena l'adozione sanzioni disciplinari nei loro confronti.

8.5. Competenze e formazioni

Ogni anno, in occasione dei colloqui individuali, il reparto delle risorse umane svolge un sondaggio tra gli addetti per valutare le loro esigenze in materia di formazione. Sulla base dei risultati viene quindi definito un programma di formazione annuale per individuare le formazioni necessarie finalizzate a colmare:

- le lacune in termini di competenze di un addetto, di un team o di un reparto;
- le esigenze di sviluppo continuo delle competenze.

Le formazioni proposte possono essere fornite internamente o da operatori esterni.

Nel corso dell'anno, delegati o esperti di cybersicurezza offrono diversi corsi tecnici, oltre a rapporti e statistiche trimestrali sulle vulnerabilità che potrebbero influire sui nostri sistemi, al fine di rafforzare le competenze del nostro personale.

8.6. Fine del contratto

È stata istituita una procedura di uscita o di risoluzione del contratto, che è stata comunicata a tutti i responsabili interessati all'interno dell'impresa. Questa procedura ha lo scopo di assicurare che il collaboratore non abbia più accesso né fisico né digitale al sistema informativo dell'impresa.

9. Gestione degli asset

9.1. Inventario

Infomaniak Network gestisce inventari degli asset essenziali e dei beni di supporto. Questi ultimi sono registrati nel nostro sistema di gestione della sicurezza delle informazioni (SMSI) e nelle nostre valutazioni dei rischi.

Esaminiamo questi asset ogni anno attraverso la SMSI e procediamo al loro aggiornamento tramite processi automatizzati in base alle esigenze dei vari team interni.

9.2. Licenze software

Infomaniak Network è impegnata a garantire l'utilizzo di licenze valide per software di terzi all'interno dei propri team interni e adotta le misure necessarie per proteggere i diritti di proprietà intellettuale.

9.3. Identificazione e classificazione degli asset

Gli asset sono segmentati, chiaramente identificati mediante una nomenclatura e una convenzione di denominazione stabilite dai team interni. Vengono eseguiti controlli continui e annuali per garantire la legittimità degli accessi, la limitazione degli accessi non autorizzati e l'affidabilità dell'inventario.

I dati sono classificati in base alle esigenze di sicurezza delle informazioni dell'organizzazione, tenendo conto dei requisiti di riservatezza, integrità e disponibilità e delle principali preoccupazioni delle parti interessate.

9.4. Aggiornamenti, antivirus e crittografia dei supporti

Il responsabile della sicurezza dei sistemi informatici (RSSI) supervisiona la protezione centrale degli asset aziendali, comprese le postazioni di lavoro degli addetti, da virus e malware. Una strategia di difesa contro tali minacce è rafforzata da un'adeguata formazione degli utenti.

La sicurezza dei supporti di archiviazione interni e rimovibili è garantita da un processo di crittografia configurato e monitorato.

Gli indicatori chiave di prestazione (KPI) sono monitorati regolarmente per verificare la conformità e la protezione degli asset.

9.5. Nomadismo

Per garantire la sicurezza delle informazioni durante il telelavoro, sono state adottate diverse precauzioni. Sono state elaborate specifiche linee guida sul telelavoro che sono state

comunicate al personale. Per connettersi alle risorse dell'organizzazione dall'esterno, è obbligatorio l'uso di una rete privata virtuale (VPN) sicura.

In tale contesto, non è inoltre consentito l'uso di dispositivi personali («Bring Your Own Device» o BYOD).

9.6. Gestione di supporti e hardware rimovibili

L'uso dei supporti rimovibili è regolato da specifiche linee guida ben note al personale. Tali istruzioni comprendono regole rigorose sul loro utilizzo, al fine di ridurre al minimo i rischi potenziali, e raccomandazioni per garantirne la protezione.

Ad esempio, può essere richiesto di crittografare i supporti rimovibili contenenti dati riservati o critici, oppure di limitarne l'uso a determinate circostanze.

9.7. Smaltimento

Per gestire gli asset sensibili dell'impresa è stata definita e attuata una politica di riciclaggio delle apparecchiature hardware e di dismissione degli asset.

Questa procedura ha lo scopo di fornire istruzioni chiare su come trattare qualsiasi tipo di hardware che memorizza dati riservati. Ciò include regole volte a garantire la distruzione sicura dei dati prima del trasferimento o dell'eliminazione dell'hardware, al fine di evitarne il successivo recupero.

10. Controllo degli accessi e gestione delle identità

10.1. Politica delle password

I collaboratori devono applicare la nostra politica di gestione delle password finalizzata a garantire la sicurezza dei nostri account e dei nostri dati per il loro intero ciclo di vita.

Ci impegniamo inoltre a informare i nostri utenti sui requisiti specifici della nostra politica delle password tenendo conto delle loro competenze, del loro ruolo e della sensibilità delle risorse a cui possono accedere.

Ecco alcuni esempi di buone pratiche consigliate nell'ambito della nostra politica delle password:

- obbligo di utilizzare un password manager autorizzato per creare e archiviare password forti;
- creare password affidabili composte da almeno dodici caratteri alfanumerici e speciali;
- evitare l'utilizzo di termini di uso comune o facilmente indovinabili;
- non condividere mai la propria password con altri e non utilizzarla per più account;

- configurare un'autenticazione a più fattori ogni volta che è possibile;

incoraggiamo tutti i nostri utenti a seguire scrupolosamente questi consigli per contribuire a mantenere un elevato livello di sicurezza all'interno della nostra organizzazione.

10.2. Gestione dei diritti

L'assegnazione degli accessi è organizzata per reparto e vengono accordate solo le autorizzazioni necessarie in base alle mansioni assegnate a ciascun soggetto.

Le domande di autorizzazione devono essere presentate attraverso canali interni predefiniti e approvate dopo un esame approfondito.

10.3. Revisione dei diritti

Il responsabile della sicurezza dei sistemi informatici e i delegati alla sicurezza effettuano una revisione annuale dei diritti di accesso.

Ogni anno vengono eseguiti controlli di sicurezza per i vari servizi interni ed esterni, i computer da ufficio, gli accessi alla rete wireless e WiFi.

La gestione avanzata degli accessi interni viene sottoposta a verifica automatica e annuale tramite strumenti interni.

10.4. Eliminazione degli accessi

L'eliminazione degli accessi degli addetti di Infomaniak Network è associata al processo HR di gestione delle entrate e delle uscite. Questo processo di uscita è rigorosamente seguito con l'ausilio di strumenti interni dedicati, sotto la direzione di responsabili designati per intraprendere le azioni necessarie.

11. Crittografia

11.1. Uso della crittografia

Sono definite e attuate regole per l'uso efficace della crittografia, compresa la gestione delle chiavi crittografiche.

Infomaniak Network ha definito e implementato una Politica di controllo crittografico e di crittografia che è stata diffusa e resa nota a tutto il suo personale.

11.2. Uso di protocolli crittografati

Infomaniak Network e i suoi collaboratori si impegnano a utilizzare i protocolli di rete protetti il più spesso possibile, sia sulle reti pubbliche come Internet che nella propria rete interna. Ad esempio, promuoviamo l'uso di HTTPS per la navigazione web, IMAPS, SMTPS o POP3S per la posta elettronica e SSH (Secure Shell) per le operazioni di amministrazione di sistema.

11.3. Mobilità

Per connettersi da remoto alla rete interna di sicurezza dell'impresa, i collaboratori dell'impresa Infomaniak Network utilizzano soltanto i loro laptop.

12. Sicurezza fisica e ambientale

12.1. Ubicazione

I data center di Infomaniak Network sono ubicati esclusivamente in Svizzera e sono interamente di proprietà dell'impresa.

12.2. Data center

12.2.1. Sicurezza fisica dei siti e controllo degli accessi

I locali sono costantemente monitorati mediante un sistema di telecamere di sorveglianza atto a impedire accessi fisici non autorizzati.

L'accesso ai data center e ai server è protetto da più barriere e da un sistema di controllo degli accessi elettronico dotato di identificazione biometrica. Per rafforzare ulteriormente la sicurezza dei data center, ogni settore e corridoio che collega i rack sono dotati di un sistema di riconoscimento facciale.

L'accesso alle sale server è limitato a un ristretto numero di addetti dell'azienda, appositamente formati e autorizzati alle aree di lavoro segmentate, in base alle esigenze specifiche dei vari team.

12.2.2. Sicurezza delle apparecchiature

I data center sono tutti certificati ISO 27001, ISO 14001 e dispongono di una ridondanza n+1 a livello di alimentazione elettrica, backbone in fibra ottica, raffreddamento, gruppi elettrogeni e inverter per garantire il funzionamento senza interruzioni delle vostre infrastrutture tecniche.

12.2.3. Sistema automatico di rilevamento, allarme ed estinzione

I nostri siti sono monitorati e dotati di sistemi di rilevamento incendi in ogni loro parte. I nostri sistemi di estinzione, calibrati per ogni tipo di ambiente di un data center, assicurano lo spegnimento automatico nelle zone in cui potrebbe scoppiare un incendio. Questi sistemi operano in locali dotati di apparecchiature elettriche, quali gli inverter, le batterie o i quadri elettrici. Questo dispositivo di monitoraggio è sempre in funzione e viene sottoposto a test continui.

12.3. Uffici

12.3.1. Sicurezza fisica dei siti e controllo degli accessi

Gli uffici della sede sociale di Infomaniak Network sono dotati di porte a chiusura automatica, accessibili soltanto tramite un sistema di badge e riconoscimento facciale: vengono effettuati regolarmente controlli degli accessi fisici.

Le telecamere di sorveglianza sono installate nei corridoi e nelle aree comuni dell'edificio, anche in prossimità delle aree di lavoro degli addetti.

12.4. Desktop vuoto e schermata vuota

Una politica di desktop vuoto e schermata vuota è in atto ed è stata comunicata a tutti gli addetti. Include istruzioni dettagliate sul blocco degli schermi, sulla corretta gestione dei documenti cartacei e digitali, sull'uso delle lavagne bianche e sulla distruzione sicura dei documenti riservati.

13. Sicurezza operativa

13.1. Monitoraggio della cybersicurezza

Le informazioni relative alle minacce in materia di sicurezza delle informazioni vengono raccolte, analizzate e trattate al fine di ottenere informazioni relative a tali minacce.

Utilizziamo un servizio di terze parti che ci offre la possibilità di monitorare le attività e le minacce presenti sul Dark Web.

La ricerca di queste potenziali minacce viene effettuata tramite parole chiave e termini specifici predeterminati, in particolare quelli legati a:

- l'esposizione degli addetti;
- il monitoraggio del marchio e dei nomi di dominio;
- il monitoraggio del Dark Net;

- l'esplorazione del deep web e la scoperta degli asset.

13.2. Dati

13.2.1. Classificazione dei dati

Le informazioni sono classificate secondo le esigenze di sicurezza delle informazioni dell'organizzazione, sulla base dei requisiti di riservatezza, integrità, disponibilità e requisiti importanti delle parti interessate.

13.2.2. Crittografia dei dati

I dati sono protetti durante il loro trasferimento tra le postazioni di lavoro degli addetti, dei clienti e il sistema informativo di Infomaniak Network grazie all'utilizzo dei protocolli di crittografia di cui al punto 11 del presente documento.

13.2.3. Integrità dei dati

Infomaniak Network si impegna a proteggere i dati dei propri clienti tramite l'adozione di procedure, misure tecniche e protocolli protetti al fine di prevenire qualsiasi alterazione, volontaria o accidentale. Ciò include solide garanzie in materia di trasmissione e conservazione delle informazioni riservate.

13.3. Gestione dei cambiamenti

La nostra politica di gestione dei cambiamenti offre agli utenti una serie di procedure operative ben documentate e controlli rigorosi su di esse. Include:

- l'inquadramento dei cambiamenti, che ne definisca chiaramente la portata e gli obiettivi;
- le linee guida da seguire per l'attuazione delle modifiche, compresi i criteri di accettazione e le norme di sicurezza;
- la pianificazione dettagliata dei cambiamenti, compresa l'individuazione dei rischi potenziali e adeguati piani di emergenza;
- il controllo rigoroso delle modifiche, con completa tracciabilità di tutte le modifiche apportate al sistema;
- processi chiari e semplici da seguire per gli aggiornamenti regolari del sistema, garantendo stabilità e prestazioni ottimali.

13.4. Protezione contro i malware

La protezione contro i malware è attuata e rafforzata da un'adeguata sensibilizzazione degli utenti. Il parco informatico delle postazioni di lavoro è monitorato da un antivirus centralizzato e controlli regolari, durante le riunioni di sicurezza vengono impostati e rivisti gli indicatori.

13.5. Politica di backup

È in vigore una politica di backup e sicurezza dei dati che definisce chiare linee guida relative al backup e al ripristino delle informazioni in conformità con gli asset identificati nel nostro sistema informativo. Questa politica specifica la durata di conservazione, la frequenza, il tipo di crittografia e i protocolli di test da seguire.

Attraverso queste misure, possiamo assicurare la protezione e il recupero efficaci dei nostri dati importanti.

13.6. Registrazione

Al nostro interno vengono generati, conservati, protetti e analizzati registri atti a registrare le attività, le eccezioni, i guasti e altri eventi rilevanti.

13.7. Sincronizzazione degli orologi

Gli orologi dei sistemi di elaborazione delle informazioni utilizzati dall'organizzazione sono sincronizzati con fonti orarie approvate.

Infomaniak Network dispone di propri server di riferimento orario che consentono a tutti i dispositivi e server di beneficiare di una sincronizzazione oraria precisa. Questo servizio è anche accessibile al pubblico e messo a disposizione sia dei clienti che dei non clienti.

13.8. Supervisione

13.8.1. Principi

Tutti i servizi e i sistemi amministrati da Infomaniak Network sono sottoposti a un attento monitoraggio. I nostri strumenti di supervisione si basano su protocolli standard e su dispositivi appositamente concepiti per raccogliere dati da tutte le fonti di controllo.

In caso di guasto, vengono emessi avvisi in tempo reale per tutti i servizi monitorati.

Questi avvisi possono anche essere inviati tramite SMS alle squadre di soccorso durante gli orari fuori ufficio.

13.8.2. Reperibilità

Il team di reperibilità assicura una sorveglianza e un intervento continui di 24 ore su 24, 7 giorni su 7 sul sistema informativo (SI) di Infomaniak Network. Il team è strutturato in diversi livelli e riunisce specialisti provenienti da diversi team di produzione, coprendo così tutte le aree di competenza.

14. Sicurezza delle comunicazioni

14.1. Architettura tecnica

L'infrastruttura che supporta i servizi di Infomaniak Network è compartimentata e strutturata in più zone di sicurezza distinte. Questa concezione offre una sicurezza rafforzata, scalabile e adeguata alle esigenze attuali e future. I gruppi di servizi informativi, di utenti e di sistemi informativi sono isolati all'interno delle reti interne all'organizzazione, garantendo così un elevato livello di protezione contro eventuali minacce esterne o interne.

14.2. Internet

Infomaniak Network dispone di propri indirizzi IP pubblici, nonché di varie connessioni Internet di provider diversi. Ciò consente all'azienda di garantire un ottimale livello di servizio ai propri clienti e addetti, anche in caso di indisponibilità di un provider. Inoltre, tutte le prestazioni gestite da Infomaniak sono dotate di ridondanza a garanzia della loro continuità.

14.3. Reti WiFi

Le reti WiFi di Infomaniak sono segmentate in base ai loro utilizzi specifici, quali ad es. le reti WiFi per ospiti, addetti, pre-produzione, ecc., con un controllo degli accessi basato sulla gestione dei diritti. I punti di accesso WiFi sono inoltre protetti per impedire accessi non autorizzati.

14.4. Equipaggiamento di sicurezza

14.4.1. Firewall

All'interno di Infomaniak sono installati dei firewall tra ogni zona di sicurezza e ogni zona applicativa. Pertanto, a garanzia di una maggiore protezione contro potenziali minacce, prima di raggiungere il servizio richiesto i flussi in entrata provenienti dall'esterno devono attraversare vari livelli di firewall.

14.4.2. IDS

In punti chiave della rete Infomaniak sono state distribuite sonde IDS per analizzare i flussi in entrata e in uscita dal sistema informativo. Tali sonde sono preposte a rilevare le attività sospette o anomale, nonché il traffico nocivo e a informare immediatamente i gruppi di produzione. A tal fine, le sonde ricevono regolarmente aggiornamenti delle firme degli attacchi dal nostro provider specializzato in cybersicurezza. L'installazione e la manutenzione di tali dispositivi sono di competenza del team di sicurezza della produzione.

14.4.3. Anti DDoS

Infomaniak implementa una protezione anti-DDoS adeguata per ciascuna delle tecnologie che utilizza assicurando così la difesa di tutte le proprie piattaforme e infrastrutture contro questo tipo di minacce informatiche. In tal modo, intende mantenere un elevato livello di disponibilità e resilienza dei propri servizi, a vantaggio della clientela e del personale.

15. Acquisizione, sviluppo e manutenzione dei sistemi informativi

15.1. Ciclo di vita di sviluppo sicuro

Norme di sicurezza, buone pratiche e buon senso sono stabilite e applicate per garantire uno sviluppo sicuro del software e dei sistemi. Tali principi comprendono:

- L'audit e la registrazione delle azioni
- La formazione degli sviluppatori in materia di sicurezza
- La lotta contro i malware
- I test di sicurezza delle applicazioni
- I test di conformità del sistema
- La sicurezza delle applicazioni Web lato client e server
- La sicurezza delle applicazioni mobili
- La crittografia

Il personale del servizio sviluppo è sensibile ai rischi legati alla sicurezza delle applicazioni e alle norme emanate dall'OWASP (Open Web Application Security Project).

Inoltre, abbiamo introdotto una politica di monitoraggio e controllo dello sviluppo esterno che raccomanda le modalità di esecuzione, le misure di sicurezza esistenti e le istruzioni imperative relative alla gestione dei log, degli accessi, del codice sorgente e ai test di sicurezza durante il ciclo di sviluppo.

15.2. Separazione degli ambienti di sviluppo, di test e operativi

Le nostre reti e infrastrutture di sviluppo sono isolate sia fisicamente che logicamente a seconda dei servizi forniti. Stiamo anche mettendo in atto una separazione distinta tra i vari ambienti applicativi, come quelli dedicati allo sviluppo, ai test, alla pre-produzione e alla produzione.

Nello specifico, l'ambiente di sviluppo è rigorosamente ristretto e accessibile agli sviluppatori solo tramite la nostra rete interna ad alta sicurezza.

16. Rapporto con i provider

Abbiamo introdotto processi e procedure finalizzati a gestire i potenziali rischi per la sicurezza delle informazioni derivanti dall'uso dei nostri prodotti o servizi presso determinati provider.

Inoltre, ci assicuriamo scrupolosamente di implementare e concordare requisiti adeguati in materia di sicurezza delle informazioni con ciascuno dei nostri provider.

Eseguiamo inoltre regolarmente una revisione, una valutazione e una gestione proattiva delle modifiche apportate alle pratiche di sicurezza delle informazioni dei nostri rispettivi provider e fornitori di servizi.

17. Gestione delle vulnerabilità e degli incidenti

17.1. Gestione delle vulnerabilità

Per quanto riguarda i team di produzione, è stato implementato un workflow per la gestione delle vulnerabilità di tipo CVE utilizzando strumenti interni e monitoraggi tecnologici.

Diversi strumenti interni consentono il monitoraggio, la sorveglianza e la scansione automatizzati delle vulnerabilità che possono influire sui nostri sistemi informativi.

Per gestire le segnalazioni di vulnerabilità è stato predisposto uno SLA (Service Level Agreement) interno, con un termine di intervento fissato in base alla gravità delle vulnerabilità individuate.

17.2. Scanner delle vulnerabilità

Vengono regolarmente effettuate analisi sui vari range di indirizzi IP Infomaniak da noi specificati. In caso di rilevamento di vulnerabilità veniamo avvisati tramite una dashboard e programmiamo dei piani d'azione per correggere rapidamente le falle individuate.

17.3. Programma di bug bounty

Collaboriamo attivamente con una comunità di ricercatori e "hacker" etici per offrire ai nostri clienti un efficace livello di sicurezza. Per testare tutti i servizi offerti ai nostri clienti sono disponibili un programma pubblico e programmi privati.

I lanciatori d'allerta beneficiano di una protezione adeguata, mentre i nostri addetti hanno la possibilità di segnalare qualsiasi irregolarità sospetta in modo confidenziale e anonimo in ogni momento.

17.4. Gestione degli incidenti di sicurezza

Una procedura consolidata di gestione degli incidenti di sicurezza definisce chiaramente i ruoli, le responsabilità, il processo di selezione, la comunicazione, la risposta e l'attenuazione, nonché l'intero flusso di lavoro necessario per garantire una risoluzione completa dell'incidente.

A seconda della gravità e della natura dell'evento, Infomaniak Network può collaborare attivamente con le autorità competenti e coordinare il processo di elaborazione dell'incidente al fine di assicurarne una risoluzione rapida ed efficace.

17.5. Gestione delle crisi

È formalizzata una procedura specifica di gestione delle crisi. Questa procedura presenta le varie fasi da seguire per risolvere l'incidente nel modo più efficace possibile e per comunicare al meglio, internamente ed esternamente, sulla causa e gli impatti.

18. Gestione della continuità operativa

18.1. Continuità del pilotaggio

Per la gestione e il pilotaggio dei servizi e delle risorse dell'infrastruttura dei nostri data center è stato definito un piano di continuità.

18.2. PCO e resilienza

La continuità operativa viene presa in considerazione a partire dalla fase di progettazione e architettura dei servizi gestiti da Infomaniak Network.

La ridondanza tra i nostri vari data center e il backup su più supporti e in più data center contribuiscono ad assicurare la continuità operativa dei nostri clienti.

Le soluzioni di disaster recovery dei nostri servizi gestiti dipendono dalle architetture tecniche e software e sono adattate al livello di ogni offerta commerciale, in base alle esigenze specifiche e ai team di produzione.

18.3. Bilancio d'impatto sull'attività

È stato configurato un Bilancio d'Impatto sull'Attività (BIA) allo scopo di raccogliere dati per pianificare e gestire efficacemente gli incidenti di sicurezza che interessano le risorse del nostro sistema informativo.

Questo BIA consente di identificare le attività e le risorse chiave dell'azienda, nonché i diversi livelli di gravità associati. Sono state inoltre definite misure specifiche per garantire la continuità operativa in caso di incidenti.

18.4. RPO e RTO

Infomaniak Network ha definito una strategia di continuità che tiene conto di tre fattori chiave:

- tempo massimo di interruzione ammissibile (TMA), conosciuto anche con il nome di Obiettivo di tempo di recupero (OTR) o Recovery Time Objective (RTO) in inglese;
- la perdita massima ammissibile di dati (PMAD), chiamata anche Obiettivo del punto di recupero (OPR) o Recovery Point Objective (RPO) in inglese;
- i potenziali impatti finanziari e commerciali.

Se pertinenti, questi elementi vengono inseriti nel Bilancio d'Impatto sull'Attività (BIA).

18.5. Piano dei test

Ogni anno viene elaborato e attuato un piano di test che tiene conto delle situazioni di rischio. Consente quanto segue:

- A monte: misurare l'efficacia del piano rispetto agli obiettivi di continuità, mediante indicatori, audit, ecc.
- Durante una crisi: monitorare i livelli di servizio effettivamente raggiunti e il funzionamento delle procedure operative previste nell'ambito del PCO.
- A posteriori: attuare un piano di miglioramento.

19. Conformità

19.1. Norme e regolamenti

19.1.1. ISO 27001

I team di Infomaniak Network svolgono le loro attività basandosi sulle norme di sicurezza riconosciute a livello internazionale, quali la ISO 27001:2022 e la ISO 27002:2022, come riferimenti per elaborare e gestire i servizi offerti ai propri clienti.

Tali norme costituiscono un solido quadro per garantire la riservatezza, l'integrità e la disponibilità dei dati sensibili e per assicurare una gestione efficace dei rischi connessi alla sicurezza delle informazioni.

19.1.2. LPD e RGPD

Infomaniak Network ha implementato un'informativa sulla privacy consultabile sul proprio sito Internet all'indirizzo: https://www.infomaniak.com/it/cgv/informativa-sulla-privacy

Inoltre, l'informativa sull'utilizzo dei cookie può essere consultata al link: https://www.infomaniak.com/it/cgv/politica-uso-cookie

19.2. Audit

19.2.1. Audit interno

Il controllo delle attività di sicurezza nei perimetri di certificazione di Infomaniak Network è assicurato da consulenti qualificati che lavorano sotto la supervisione del team di conformità.

Questi consulenti eseguono regolarmente un esame degli elementi associati ai perimetri certificati, conformemente al piano di audit e alla dichiarazione di applicabilità di Infomaniak Network.

I documenti relativi agli audit interni sono riservati e non possono essere divulgati.

19.2.2. Audit esterno

Nell'ambito della certificazione ISO 27001:202, Infomaniak Network viene sottoposta ad audit annuale da parte degli enti di certificazione.

19.2.3. Audit tecnico

Infomaniak Network si avvale di esperti qualificati per effettuare audit tecnici regolari sul proprio sistema informativo e in base alle esigenze e per la produzione di nuovi servizi.

19.2.4. Audit cliente

I clienti hanno la possibilità di effettuare test di penetrazione (pentests) sui servizi che utilizzano, nel rigoroso rispetto delle condizioni specificate nel contratto.

Devono inoltre tenere conto dei vincoli dei team interni, come l'esecuzione dei pentests solo durante l'orario d'ufficio e informando preventivamente i team di produzione.