

Politica della qualità e della sicurezza delle informazioni

Sommario

1.	<u>INTRODUZIONE</u>	3
1.1	<u>PREMESSE E PERIMETRO APPLICATIVO DELLA NORMA</u>	3
1.2	<u>OBIETTIVI DEL RGS</u>	5
1.3	<u>TERMINI E DEFINIZIONI</u>	6
1.4	<u>RIFERIMENTI NORMATIVI</u>	7
1.4.1	VIGENTI NORME DI LEGGE	7
1.4.2	NORME DI STANDARDIZZAZIONE COMUNITARIE ED INTERNAZIONALI DI RIFERIMENTO	7
1.4.3	DOCUMENTI DEL SGSI	7
1.4.4	DOCUMENTI DEL SISTEMA DI GESTIONE PER LA QUALITÀ	7
2.	<u>POLICY</u>	7
2.1	<u>PRINCIPI GENERALI</u>	7
2.2	<u>IDENTIFICAZIONE, CLASSIFICAZIONE E GESTIONE DELLE RISORSE</u>	8
2.2.1	DOCUMENTAZIONE DI SISTEMA:	8
2.3	<u>GESTIONE SICURA DEGLI ACCESSI LOGICI:</u>	8
2.3.1	DOCUMENTAZIONE DI SISTEMA:	9
2.4	<u>NORME COMPORTAMENTALI PER LA GESTIONE SICURA DELLE RISORSE AZIENDALI:</u>	9
2.4.1	NORMATIVA NAZIONALE:	9
2.4.2	DOCUMENTAZIONE DI SISTEMA:	9
2.5	<u>PERSONALE E SICUREZZA:</u>	10
2.5.1	DOCUMENTAZIONE DI SISTEMA:	10
2.6	<u>GESTIONE DEGLI EVENTI ANOMALI E DEGLI INCIDENTI:</u>	10
2.6.1	DOCUMENTAZIONE DI SISTEMA:	10
2.7	<u>GESTIONE DELLA SICUREZZA FISICA:</u>	11
2.7.1	DOCUMENTAZIONE DI SISTEMA:	11
2.7.2	ASPETTI LEGATI AL CAMBIAMENTO CLIMATICO:	11
2.8	<u>GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI PER I SERVIZI CLOUD</u>	12
2.9	<u>ASPETTI CONTRATTUALI CONNESSI ALLA SICUREZZA DELLE INFORMAZIONI</u>	12
2.9.1	NORMATIVA NAZIONALE:	12
2.9.2	DOCUMENTAZIONE DI SISTEMA:	13
2.10.1	DOCUMENTAZIONE DI SISTEMA:	13
2.11	<u>MONITORAGGIO, TRACCIAMENTO E VERIFICHE TECNICHE</u>	13
2.11.1	DOCUMENTAZIONE DI SISTEMA:	14
2.12	<u>CICLO DI VITA DEI SISTEMI E DEI SERVIZI</u>	14
2.13	<u>RISPETTO DELLA NORMATIVA</u>	15
2.13.1	DOCUMENTAZIONE DI SISTEMA:	15

<u>2.14 SICUREZZA DEI DATI DEI CLIENTI GESTITI TRAMITE I SERVIZI SAAS VENDUTI</u>	15
<u>3. DEFINIZIONE DEI RUOLI E DELLE RESPONSABILITÀ</u>	15
<u>3.1 STRUTTURA RESPONSABILE DELLA GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI</u>	15
<u>3.1.1 DOCUMENTAZIONE DI SISTEMA:</u>	16
<u>3.2 MANAGEMENT E FUNZIONE SEC</u>	16

1. Introduzione

Il presente documento pubblico è messo a disposizione dei clienti Axios Italia Service S.r.l. al fine di rendere pubbliche le politiche che mirano a garantire la sicurezza delle informazioni gestite per conto dei propri clienti.

1.1 Premesse e perimetro applicativo della norma

Lo scopo del presente documento (di seguito indicato come Politica per la Sicurezza delle Informazioni) è quello di descrivere i principi generali di sicurezza delle informazioni che Axios Italia ha fatto propri, al fine di realizzare e mantenere un efficiente e sicuro Sistema di Gestione per la qualità e della Sicurezza delle Informazioni ai sensi delle norme ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018 e UNI EN ISO 9001.

Tali principi sono concretizzati nelle Procedure, Istruzioni Operative, Regolamenti e nella ulteriore documentazione, interna ed esterna, in utilizzo aziendale ai fini della tutela della sicurezza delle informazioni e in relazione alle reali esigenze derivanti dalla tipologia di attività svolte da Axios nello specifico ambito di applicazione della suddetta norma.

L'ambito di applicazione del Sistema di gestione per la qualità e della Sicurezza delle Informazioni e della presente Politica e dell'infrastruttura, intesa in senso fisico e logico-informatico del Centro progettazione, sviluppo, manutenzione e assistenza di software gestionale: Via Emanuele Filiberto – 190 00185 Roma.

Nella suddetta infrastruttura sono ospitati, in ambienti dotati di idonee misure di sicurezza infrastrutturali sia fisiche che logico-informatiche, sistemi ed apparecchiature di elaborazione/gestione dati (genericamente server”).

I suddetti locali garantiscono anche i seguenti servizi strumentali (c.d. “facilities”):

- Sistema di controllo degli accessi
- Sistema di alimentazione elettrica diretta (sistema alimentazione primario) ed indiretta (sistemi di alimentazione di back up – gruppo di continuità)
- Sistema di condizionamento ambientale
- Sistema antincendio
- Sistemi di protezione logico informatica (firewalling – antivirus – etc.)

Quanto successivamente descritto nel presente documento e nella ulteriore documentazione di riferimento per il Sistema di Gestione della Sicurezza delle Informazioni, deve essere inteso, dunque, come applicato esclusivamente al suddetto perimetro fisico-logico nonché ai processi, risorse e/o rapporti lavorativi (Personale dipendente/Collaboratori/Terzi aventi causa) correlati e/o connessi alla debita gestione in esercizio della suddetta infrastruttura nell'ambito dei più ampi e generali scopi aziendali.

Axios Italia fonda la propria organizzazione sui seguenti principi:

- Rispetto della legislazione vigente;
- Conformità del sistema di gestione;
- Competenza, professionalità ed imparzialità del personale;

- Coinvolgimento del personale nell'implementazione e nel miglioramento del sistema di gestione per la qualità;
- Adeguatezza della struttura e delle attrezzature;
- Erogazione dei servizi nel rispetto della normativa per la certificazione, della legislazione di riferimento e dei requisiti dei clienti;
- Aggiornamento tecnico del personale e delle attrezzature;
- Adeguatezza dell'organizzazione e del sistema di gestione per la qualità alle esigenze interne e del mercato.

L'operato della Axios Italia rispetta i seguenti principi:

- Collaborazione con gli Enti di certificazione;
- Collaborazione con i clienti.

L'Alta Direzione inoltre:

- Fa in modo di rendere disponibili le risorse necessarie a garantire l'efficacia del Sistema di Gestione per la Qualità e sicurezza delle informazioni;
- Comunica ed aggiorna ogni anno gli orientamenti, gli impegni e gli obiettivi per la qualità;
- Convoca periodicamente specifiche riunioni, affinché ad ogni livello sia nota e condivisa la necessità di soddisfare i requisiti previsti dai contratti e capitolati e per effettuare gli aggiornamenti richiesti dall'evoluzione delle norme cogenti;
- Garantisce che gli obiettivi della politica di qualità siano definiti e compatibili con il contesto e la direzione strategica della società e che comprendano la sicurezza delle informazioni;
- Garantisce l'integrazione dei requisiti di sistema di gestione integrato nei processi di business aziendali;
- Promuove l'uso dell'approccio per processi e il pensiero basato sul rischio;
- Provvede affinché le risorse necessarie per il sistema di gestione della qualità siano disponibili;
- Assicura che il sistema di gestione integrato raggiunga i risultati attesi;
- Coinvolge, dirige e sostiene il personale al fine di ottenere l'efficacia del sistema di gestione;
- Promuove il miglioramento;
- Fa in modo che la Politica aziendale sia comunicata e condivisa con tutti i dipendenti. L'Alta Direzione si impegna inoltre a:

Divulgare e promuovere la politica per la qualità;

Attuare la politica per la qualità attraverso la definizione di obiettivi di miglioramento;

Riesaminare la politica per la qualità in funzione dei risultati raggiunti e delle strategie aziendali.

Con l'integrazione del Sistema di Gestione per la qualità e Sicurezza delle Informazioni Axios Italia si prefigge la finalità di proteggere da tutte le minacce, interne o esterne, intenzionali o accidentali, il patrimonio informativo aziendale, ivi comprese le informazioni e i dati relativi a clienti e fornitori, oltre a mantenere e dimostrare la correttezza delle trattative con clienti e fornitori e di dare evidenza che i servizi erogati non causino direttamente o indirettamente un aumento dei rischi per i clienti.

Per il perseguimento di tali finalità, la Società ha individuato nella documentazione del Sistema di Gestione Integrato le modalità di valutazione e i criteri di gestione dei rischi, valutando gli

investimenti economici che l'implementazione e il mantenimento del Sistema di Gestione potrà comportare.

Pertanto, la Direzione si impegna, nel rispetto dei requisiti cogenti, ad assicurare che:

- Le informazioni siano protette da accessi non autorizzati nel rispetto della riservatezza e siano disponibili solo agli utenti autorizzati;
- Le informazioni non vengano divulgate a persone non autorizzate a seguito di azioni deliberate o per negligenza e, nel rispetto dell'integrità, siano salvaguardate da modifiche non autorizzate;
- Vengano predisposti piani per la continuità dell'attività aziendale e che tali piani siano il più possibile tenuti aggiornati e controllati;
- Il personale riceva addestramento sulla sicurezza delle informazioni;
- Tutte le violazioni della sicurezza delle informazioni e possibili punti deboli vengano riferiti a chi di dovere ed esaminati.

Attraverso l'attuazione di tale politica Axios Italia intende ottemperare all'impegno di conformità alla ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018 e UNI EN ISO 9001 nonché di conseguire e mantenere tale certificazione. Per il conseguimento di tale obiettivo, la direzione si impegna a far sì che la presente politica sia diffusa, compresa e attuata non solo dal personale interno, ma anche da collaboratori esterni e fornitori che siano in qualsiasi modo coinvolti con le informazioni aziendali.

La Direzione si impegna infine a riesaminare regolarmente la politica ed eventuali modifiche o cambiamenti che la influenzino in ambito organizzativo, per accertarsi che permanga idonea all'attività e alla capacità di soddisfare i Clienti, i Fornitori e le altre parti interessate. Il riesame della stessa sarà comunque effettuato a seguito dell'annuale Riesame della Direzione.

1.2 Obiettivi del RGSI

La sicurezza delle informazioni ha come obiettivo primario la protezione dei dati e degli elementi del sistema informativo responsabile della loro gestione.

In particolare, perseguire la sicurezza delle informazioni significa definire, conseguire e mantenere le seguenti proprietà delle stesse:

- **Riservatezza:** assicurare che l'informazione sia accessibile solamente ai soggetti e/o ai processi debitamente autorizzati;
- **Integrità:** salvaguardare la consistenza dell'informazione da modifiche non autorizzate;
- **Disponibilità:** assicurare che gli utenti autorizzati abbiano accesso alle informazioni e agli elementi architetture associati quando ne fanno richiesta;
- **Autenticità:** garantire la provenienza dell'informazione;
- **Non ripudio:** assicurare che l'informazione sia protetta da falsa negazione di ricezione, trasmissione, creazione, trasporto e consegna.

La mancanza di adeguati livelli di sicurezza, in termini di Riservatezza, Disponibilità, Integrità, Autenticità e Non Ripudio, può comportare, nell'ambito di una qualsiasi attività aziendale, il danneggiamento dell'immagine aziendale, la mancata soddisfazione del cliente, il rischio di incorrere in sanzioni legate alla violazione delle normative vigenti nonché danni di natura economica e finanziaria.

La sicurezza delle informazioni è, quindi, un requisito fondamentale per garantire l'affidabilità delle informazioni trattate, nonché l'efficacia ed efficienza dei servizi erogati da Axios Italia. Di conseguenza, è essenziale per la società identificare le esigenze di sicurezza sia di natura esterna che derivanti dal cogente.

Tale attività viene realizzata attingendo a diverse fonti:

Analisi dei rischi: consente all'azienda di acquisire la consapevolezza e la visibilità sul livello di esposizione al rischio del proprio sistema informativo. Sulla base di tale livello sono individuate le misure di sicurezza idonee. La valutazione del rischio consiste nella sistematica considerazione dei seguenti elementi:

- Danno che può derivare dalla mancata applicazione di misure di sicurezza al sistema informativo, considerando le potenziali conseguenze derivanti dalla perdita di riservatezza, integrità, disponibilità, autenticità e non ripudio delle informazioni;
- Realistica probabilità di come sia possibile perpetrare un attacco alla luce delle minacce individuate.

I risultati della valutazione aiutano a determinare quali siano le azioni necessarie per gestire i rischi individuati e le misure di sicurezza più idonee rispetto ai propri obiettivi, in base alla definizione del livello di rischio residuo che l'azienda decide di accettare, da implementare successivamente.

Principi ispiratori: Rappresentano il sistema dei valori in cui l'azienda crede con riferimento alla gestione della sicurezza del proprio sistema informativo. Si tratta delle idee di fondo che l'azienda ha maturato nei riguardi della sicurezza delle informazioni, ovvero che cosa sia giusto fare, o meno, per disporre di un sistema di gestione della sicurezza efficiente, efficace e adeguato alle proprie necessità. Il riferimento primario dei principi generali di sicurezza è lo standard ISO/IEC 27001:2022.

Leggi e contratti: nell'ambito del contesto normativo esistente, vengono fornite indicazioni su come affrontare le problematiche della sicurezza e su come gestire l'utilizzo dei sistemi informativi. Il rispetto della legislazione italiana relativa alla sicurezza serve, oltre che per limitare i rischi di un coinvolgimento dell'azienda, anche per garantire un livello minimo di sicurezza del sistema informativo da proteggere.

La presente policy, nel rispetto delle principali norme e degli standard in materia:

- Sottolinea l'importanza di garantire la sicurezza delle informazioni e degli strumenti atti al trattamento delle stesse;
- È coerente con la volontà espressa dalla società di garantire la protezione del patrimonio informativo;
- Ha come oggetto aspetti fisici, logici ed organizzativi del Sistema di Gestione della Sicurezza delle Informazioni.

1.3 Termini e definizioni

- **Asset o Bene:** Qualsiasi risorsa che abbia un valore per l'organizzazione, sia essa materiale che immateriale (es. beni fisici, software, informazioni e dati, ...).

- **Autenticità:** Proprietà per la quale è garantito che l'identità di un soggetto o di una risorsa è quella dichiarata; l'autenticità si applica ad entità quali utenti, processi, sistemi ed informazioni.
- **Disponibilità:** Proprietà per la quale le informazioni sono rese accessibili ed utilizzabili su richiesta di un'entità autorizzata.
- **Integrità:** Proprietà per la quale l'accuratezza e la completezza degli asset è salvaguardata.
- **Non ripudio:** Capacità di dimostrare che un'azione o un evento hanno avuto luogo, in modo che questo evento od azione non possano essere ripudiati successivamente.
- **Riservatezza:** Proprietà per la quale le informazioni non sono rese disponibili o divulgate a individui, entità o processi non autorizzati.
- **Hardening:** Insieme di azioni atte ad analizzare le funzionalità di un sistema operativo/applicazione al fine di individuare la configurazione ottima che permetta di innalzare il livello di sicurezza e ridurre il rischio residuo connesso alle debolezze dei sistemi.

1.4 Riferimenti normativi

1.4.1 *Vigenti norme di legge*

“Codice in materia di protezione dei dati personali”

REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI

Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016

1.4.2 *Norme di standardizzazione comunitarie ed internazionali di riferimento*

ISO/IEC 27001

ISO/IEC 27017

ISO/IEC 27018

UNI EN ISO 9001

1.4.3 *Documenti del SGSI*

L'elenco generale dei documenti comprensivo della eventuale categoria di classifica è conservato nell'archivio qualità.

1.4.4 *Documenti del Sistema di Gestione per la Qualità*

Procedure

Istruzioni

Moduli

2. Policy

2.1 Principi generali

I principi generali ai quali Axios Italia ispira la sua Politica di Gestione della Sicurezza delle Informazioni, nello specifico perimetro applicativo della norma sono articolati nelle seguenti tematiche:

- Identificazione, classificazione e gestione delle risorse
- Gestione sicura degli accessi logici
- Norme comportamentali per la gestione sicura delle risorse aziendali
- Personale e Sicurezza
- Gestione degli eventi anomali e degli incidenti
- Gestione della sicurezza fisica
- Aspetti contrattuali connessi alla sicurezza delle informazioni
- Gestione della Business Continuity
- Monitoraggio, tracciamento e verifiche tecniche
- Ciclo di vita dei sistemi e dei servizi
- Rispetto della normativa
- Aspetti legati al cambiamento climatico

Di seguito, si riporta, per ciascuna tematica, l'obiettivo e le linee guida definite da Axios Italia.

2.2 Identificazione, classificazione e gestione delle risorse

Obiettivo: *garantire la piena conoscenza delle informazioni gestite in Axios Italia e la valutazione della loro criticità, al fine di agevolare l'implementazione degli adeguati livelli di protezione.*

- Deve esistere ed essere mantenuto aggiornato, nel corso del tempo, un sistema di censimento di tutti i beni materiali ed immateriali da tutelare (informazioni, hardware, software, documentazioni cartacee e supporti di memorizzazione);
- Ogni risorsa (bene materiale/immateriale) deve essere direttamente associabile ad una Funzione aziendale responsabile.
- Le informazioni devono essere classificate in base al loro livello di criticità, in modo da essere gestite con livelli di riservatezza ed integrità coerenti ed appropriati. La criticità delle informazioni deve essere valutata in maniera quanto più oggettiva possibile, attraverso l'utilizzo di adeguate metodologie di lavoro.
- Le modalità di gestione ed i sistemi di protezione per le informazioni e gli asset su cui risiedono devono essere coerenti con il livello di criticità identificato.

2.2.1 Documentazione di Sistema:

- Politica della sicurezza delle informazioni
- Elenco e piano di continuità operativa
- Classificazione Informazioni

2.3 Gestione sicura degli accessi logici:

Obiettivo: *garantire l'accesso sicuro alle informazioni, in modo da prevenire trattamenti non autorizzati delle stesse o la loro visione da parte di utenti che non hanno i necessari diritti.*

- L'accesso alle informazioni da parte di ogni singolo utente deve essere limitato alle sole informazioni di cui necessita per lo svolgimento dei propri compiti (c.d. principio del "need-to-know"). La comunicazione e trasmissione di informazioni all'interno, così come verso l'esterno, deve fondarsi sullo stesso principio.

- L'accesso alle informazioni in formato digitale da parte di utenti e sistemi autorizzati deve essere subordinato al superamento di una procedura di identificazione ed autenticazione degli stessi.
- Le autorizzazioni di accesso alle informazioni devono essere differenziate in base al ruolo ed agli incarichi ricoperti dai singoli individui e devono essere periodicamente sottoposte a revisione.
- È necessario definire un processo di gestione delle credenziali di autorizzazione e dei relativi profili di accesso.
- I sistemi che costituiscono l'infrastruttura devono essere opportunamente protetti e segregati, in modo da minimizzare la possibilità degli accessi non autorizzati.

2.3.1 Documentazione di Sistema:

- Gestione Credenziali
- Organigramma funzionale Axios Italia
- Mansionario funzionale Axios Italia
- Regolamento aziendale

2.4 Norme comportamentali per la gestione sicura delle risorse aziendali:

Obiettivo: *garantire che i dipendenti e collaboratori di Axios Italia adottino modelli di comportamento volti a garantire adeguati livelli di sicurezza delle informazioni.*

- Gli ambienti di lavoro e le risorse aziendali devono essere utilizzati in modo congruo con le finalità per le quali sono state rese disponibili e garantendo la sicurezza delle informazioni trattate.
- Devono essere definite delle procedure per la gestione ed utilizzo delle informazioni sia su supporto digitale che su supporto cartaceo.
- I sistemi informatici aziendali devono essere impiegati da dipendenti e da collaboratori secondo procedure approvate.

2.4.1 Normativa nazionale:

CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

D.lgs. n.196/03 come modificato dal D.lgs. 101/2018 e ss. mm. e ii.

REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI

Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016

2.4.2 Documentazione di Sistema:

- Politica della sicurezza delle informazioni (il presente documento)
- Classificazione Informazioni
- Regolamento aziendale
- Gestione credenziali

2.5 Personale e sicurezza:

Obiettivo: *garantire che il personale che opera per conto di Axios Italia (dipendenti e collaboratori), abbia piena consapevolezza delle problematiche relative alla sicurezza delle informazioni.*

- Nelle fasi di selezione ed inserimento del personale in Axios Italia devono essere valutati i livelli di conoscenza degli obiettivi e delle problematiche di sicurezza aziendale in funzione delle attività che dovranno essere svolte.
- Durante la permanenza in Axios Italia il personale deve ricevere un'adeguata e continuativa formazione inerente le tematiche di sicurezza dei dati.
- Le modalità di chiusura del rapporto di lavoro con Axios Italia dovranno essere coerenti con gli obiettivi di sicurezza aziendale

2.5.1 Documentazione di Sistema:

- Politica della sicurezza delle informazioni (il presente documento)
- Classificazione Informazioni
- Regolamento aziendale
- Organigramma funzionale Axios Italia
- Mansionario funzionale Axios Italia
- Piano di formazione aziendale

2.6 Gestione degli eventi anomali e degli incidenti:

Obiettivo: *garantire che le anomalie e gli incidenti aventi ripercussioni sul sistema informativo e sui livelli di sicurezza aziendale siano tempestivamente riconosciuti e correttamente gestiti attraverso efficienti sistemi di prevenzione, comunicazione e reazione al fine di minimizzare l'impatto sul business.*

- Tutti i dipendenti e i collaboratori sono tenuti a rilevare e notificare, a chi di competenza e secondo adeguate procedure, eventuali problematiche legate alla sicurezza delle informazioni.
- Gli incidenti che possono avere un impatto sui livelli di sicurezza devono essere rilevati e gli eventuali danni, potenziali e no, devono essere gestiti, ove possibile, in tempi brevi secondo specifiche procedure.
- Deve esistere un sistema di registrazione e classificazione degli incidenti e degli eventi anomali per effettuare analisi volte al miglioramento dei livelli di sicurezza coerentemente con le reali problematiche riscontrate.

2.6.1 Documentazione di Sistema:

- Gestione degli incidenti di sicurezza informatica
- Procedura di *Data breach*

2.7 Gestione della sicurezza fisica:

Obiettivo: *prevenire l'accesso non autorizzato alle sedi ed ai singoli locali aziendali e garantire adeguati livelli di sicurezza alle aree e agli asset mediante i quali vengono gestite le informazioni.*

- Deve essere garantita la gestione della sicurezza delle aree e dei locali tramite:
 - L'individuazione delle aree e la classificazione dei locali in base alla criticità delle informazioni elaborate;
 - La definizione dei livelli adeguati di protezione;
 - La predisposizione di un ciclo periodico di verifiche e controlli.
- Deve essere garantita la sicurezza delle apparecchiature tramite:
 - La definizione di un'adeguata collocazione delle apparecchiature per l'elaborazione delle informazioni;
 - La messa a disposizione delle risorse necessarie al loro funzionamento;
 - La predisposizione di un adeguato livello di manutenzione;
 - La predisposizione di un ciclo periodico di verifiche e controlli.

2.7.1 Documentazione di Sistema:

- Elenco asset e piano continuità operativa
- Elenco e registrazione controlli
- Backup
- Rispristino
- Sistemi monitoraggio

2.7.2 Aspetti legati al cambiamento climatico:

Axios considera i rischi ambientali e le opportunità legate al cambiamento climatico e si impegna a sviluppare strategie per migliorare la resilienza alle interruzioni della catena di fornitura, conformarsi alle normative emergenti, e rispondere alle aspettative crescenti di clienti e altre parti interessate per pratiche sostenibili.

2.8 Gestione della sicurezza delle informazioni per i servizi cloud

Cliente servizio Cloud (Axios)	Fornitore di servizi di cloud
Axios nella definizione degli accordi con il fornitore di servizi cloud prende in considerazione i seguenti aspetti: - Informazioni memorizzate in ambiente di cloud computing possono essere oggetto di accesso e di gestione da parte del fornitore di servizi di cloud; - I beni possono essere mantenuti in ambiente cloud computing, ad esempio, i programmi applicativi; - I processi possono essere eseguiti su un multi-conduttore, servizio cloud virtuale; - Gli amministratori di servizi cloud hanno accesso privilegiato; - Le aree geografiche di organizzazione del fornitore di servizi di cloud e dei paesi in cui il fornitore di servizi di cloud in grado di memorizzare i dati dei clienti di servizi cloud (anche solo temporaneamente).	Axios chiede garanzia al fornitore di servizi Cloud in merito ai seguenti aspetti: - Rischi da addetti ai lavori autorizzati - L'accesso alle attività di servizi cloud dei clienti da parte del personale del prestatore di servizi di cloud - garanzia in merito alle procedure di controllo di accesso - Pronta comunicazioni durante la gestione del cambiamento - La garanzia della protezione dei dati - La gestione del ciclo di vita dei dati - La comunicazione di violazioni

2.9 Aspetti contrattuali connessi alla sicurezza delle informazioni

Obiettivo: *assicurare la conformità con i requisiti legali e con i principi legati alla sicurezza delle informazioni nei contratti con le terze parti, in accordo con le caratteristiche specifiche della relazione che Axios Italia deve instaurare con le terze parti stesse.*

- Gli accordi con le terze parti e con gli outsourcer che accedono alle informazioni e/o agli strumenti che le elaborano, devono essere basati su contratti formali contenenti opportuni requisiti di sicurezza.
- Gli accordi con terze parti e con gli outsourcer, ove necessario, devono garantire il rispetto dei requisiti di legge in materia di protezione dei dati personali (“normativa privacy”).

2.9.1 Normativa nazionale:

CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

D.lgs. n.196/03 come modificato dal D.lgs. 101/2018 e ss. mm. e ii.

REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI

Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016

2.9.2 Documentazione di Sistema:

- Contratto Quadro Appalti - Atti d'affido
- Addendum ex art.28 Regolamento UE 2016/679 (incarico al Responsabile/Sub-responsabile del trattamento) basato sulle SCC (EDPB) da utilizzare per i contratti tra Titolari e Responsabili del trattamento (Responsabile e Sub-responsabile del trattamento).

2.10 Gestione della Business Continuity

Obiettivo: *garantire la continuità dell'attività di Axios Italia e l'eventuale ripristino tempestivo dei servizi erogati colpiti da eventi anomali di una certa gravità, riducendo le conseguenze sia all'interno che all'esterno del contesto aziendale.*

- Devono essere attentamente identificati e valutati, in termini di probabilità di accadimento e possibili conseguenze, tutti gli eventi da cui può dipendere un'interruzione della continuità del business.
- Deve essere predisposto un piano di continuità che permetta all'organizzazione di affrontare, in modo organizzato ed efficiente, le conseguenze di un evento imprevisto garantendo il ripristino dei servizi critici in tempi e con modalità che consentano la riduzione delle conseguenze negative sulla missione aziendale.
- Devono essere preparate, validate e opportunamente divulgate tutte le procedure operative ed organizzative necessarie per assicurare l'implementazione del piano di continuità.
- Devono essere periodicamente effettuati i test per tutti i componenti del piano di continuità.
- Deve essere assicurato il mantenimento e l'aggiornamento dei piani e delle procedure di cui ai punti precedenti al fine di garantire l'efficacia del sistema nel tempo a fronte di eventuali cambiamenti organizzativi/tecnologici.

2.10.1 Documentazione di Sistema:

- Elenco asset e piano continuità operativa
- Business Continuity Planning
- Backup
- Ripristino
- Procedura Gestione Incidenti Sicurezza
- Gestione degli incidenti di sicurezza informatica

2.11 Monitoraggio, tracciamento e verifiche tecniche

Obiettivo: *garantire la rilevazione di eventi anomali, incidenti e vulnerabilità dei sistemi informativi al fine di assicurare la sicurezza e la disponibilità dei servizi e delle relative informazioni.*

- I sistemi informativi devono essere periodicamente controllati in modo da valutare il corretto funzionamento dei sistemi di sicurezza, hardware e software, implementati, nonché l'eventuale presenza di vulnerabilità non riscontrate o conosciute in passato.

- A fronte dei risultati di tutte le attività di monitoraggio, tracciamento e verifica devono essere effettuate periodiche attività di analisi, volte all'identificazione delle aree critiche e delle opportune azioni correttive e migliorative.
- Devono essere pianificate attività periodiche di audit del sistema di gestione della sicurezza delle informazioni.

2.11.1 Documentazione di Sistema:

- Piano Audit
- Business Continuity Planning
- Backup
- Rispristino

2.12 Ciclo di vita dei sistemi e dei servizi

Obiettivo: *assicurare che gli aspetti di sicurezza siano inclusi in tutte le fasi di progettazione, sviluppo, esercizio, manutenzione, assistenza e dismissione dei sistemi e dei servizi informatici.*

- Nella fase di progettazione e sviluppo devono essere opportunamente considerati gli aspetti di sicurezza. In particolare, devono essere indirizzate le seguenti tematiche:
 - Inclusione dei requisiti di sicurezza nelle specifiche funzionali dei servizi e sistemi;
 - Adozione di best practice per lo sviluppo e la manutenzione del software;
 - Gestione controllata della documentazione;
 - Separazione degli ambienti di sviluppo e test con impiego di procedure formali di accettazione nel passaggio fra ambienti.
- Nella fase di esercizio devono essere opportunamente considerati gli aspetti di sicurezza. In particolare, devono essere indirizzate le seguenti tematiche:
 - Adozione di procedure di backup e restore;
 - Adozione di procedure di dismissione controllata dei sistemi (per esempio cancellazione sicura dei dischi);
 - Network security: segregazione delle reti, monitoraggio dei gateway (firewall).
- Nella gestione dei servizi devono essere opportunamente considerati gli aspetti di sicurezza. In particolare, devono essere indirizzate le seguenti tematiche:
 - Monitoraggio dei sistemi e servizi;
 - Gestione utenze;
 - Performance monitoring.

2.13 Rispetto della Normativa

Obiettivo: *garantire il rispetto delle disposizioni di legge, di statuti, regolamenti o obblighi contrattuali e di ogni requisito inerente alla sicurezza delle informazioni, riducendo al minimo il rischio di sanzioni legali o amministrative, di perdite rilevanti o danni di reputazione.*

- Tutti i requisiti normativi e contrattuali in materia di sicurezza del sistema informativo e aventi impatto sul Sistema di Gestione della Sicurezza delle Informazioni devono essere identificati ed analizzati, al fine di valutarne gli impatti sull'organizzazione e sui sistemi informativi.
- I responsabili delle diverse aree devono assicurarsi, ciascuno nell'ambito di propria competenza, che tutte le politiche, le procedure, gli standard e in generale tutta la documentazione relativa alla sicurezza delle informazioni siano applicati e rispettati.
- Il mancato rispetto di quanto indicato in questo documento, e in tutti gli altri che da esso discendono, sarà gestito in ottemperanza a quanto previsto nel CCNL oppure, nel caso di inadempienze di terze parti, secondo i rapporti contrattuali in essere.

2.13.1 Documentazione di Sistema:

- Condizioni Generali di contratto
- Condizioni Particolari di contratto Hosting, Domini, Mail
- Condizioni Particolari di contratto Housing
- Condizioni Particolari di contratto Telefonia e Comunicazione elettronica
- Addendum ex art.28 Regolamento UE 2016/679 (incarico al Responsabile/Sub-responsabile del trattamento) basato sulle SCC (EDPB) da utilizzare per i contratti tra Titolari e Responsabili del trattamento (Responsabile e Sub-responsabile del trattamento).
-

2.14 Sicurezza dei dati dei clienti gestiti tramite i servizi SaaS venduti

L'azienda ha sempre fatto della sicurezza delle informazioni e della salvaguardia delle stesse un fiore all'occhiello dei propri sistemi. Oltre a tutti i sistemi di protezione dei dati da attacchi esterni, backup degli stessi e sistemi di disaster recovery all'avanguardia, Axios ha deciso di adottare, al fine di tutelare le informazioni di accesso dei propri utenti, un sistema di hashing che consente di non memorizzare le credenziali di accesso dell'utente ma solo di effettuare una verifica sulla bontà delle stesse. I criteri adottati sono quelli suggeriti da ACN nel documento relativo alle Linee guida sui criteri di conservazione delle password.

3. Definizione dei ruoli e delle responsabilità

3.1 Struttura responsabile della gestione della sicurezza delle informazioni

La struttura responsabile del sistema di gestione della sicurezza delle informazioni dovrà farsi promotrice, al fine di rendere la politica generale di sicurezza coerente con l'evoluzione del contesto aziendale, delle eventuali azioni da intraprendere a fronte del verificarsi di eventi quali:

- Nuove minacce o modifiche a quelle considerate nelle precedenti attività di analisi del rischio;
- Significativi incidenti di sicurezza;

- Evoluzione del contesto normativo e legislativo in materia di sicurezza delle informazioni;
- Risultati di analisi sui costi, impatti, efficacia ed efficienza del sistema di gestione per la sicurezza delle informazioni.

3.1.1 Documentazione di Sistema:

- Procedura Gestione Incidenti Sicurezza
- Gestione degli incidenti di sicurezza informatica
- Organigramma funzionale Axios Italia
- Mansionario funzionale Axios Italia

3.2 Management e Funzione SEC

Il Management (Direzione) è la funzione aziendale apicale a cui competono, con il supporto della funzione direzionale principale SEC (Security), della struttura responsabile del sistema di gestione della sicurezza delle informazioni (RGSI) e del DPO (RPD), le decisioni di massimo livello riguardo alle tematiche di sicurezza.

In particolare, ha la responsabilità di supportare e garantire, mediante le funzioni aziendali subordinate, l'applicazione delle politiche generali del Sistema di Gestione della Sicurezza delle Informazioni, di definire le politiche idonee di gestione del rischio e di supportare costantemente il processo di sensibilizzazione sulle tematiche di sicurezza.

Axios Italia Service S.r.l.
L'amministratore unico
Eleonora Iommi