ATUMTEK
THE INNOVATION GROUP
info@atumtek.it | www.Atumtek.it

PO 01
POLITICA PER LA SICUREZZA DELLE INFORMAZIONI

Versione	Data	Descrizione	Emesso	Verificato	Approvato
1	31/10/2024	Prima emissione	Massimiliano GRIMOLDI	Gabriele BROGNOLI	Vincenzo MADE'
2	16/06/2025	Prima revisione	Massimiliano GRIMOLDI	Vincenzo MADE'	Vincenzo MADE'
3	25/08/2025	Seconda revisione	Massimiliano GRIMOLDI	Vincenzo MADE'	Vincenzo MADE'
4	29/05/2026	Terza revisione	Massimiliano GRIMOLDI	Vincenzo MADE'	Vincenzo MADE'

Lista di distribuzione

Il presente documento è stato distribuito a tutti i dipendenti e collaboratori tramite pubblicazione all'interno di una cartella di rete condivisa. Tale pubblicazione è stata comunicata tramite mail a tutti i destinatari.

INDICE

Elenco Tabelle

Elenco Figure

Non è stata trovata alcuna voce dell'indice delle figure.

1 INTRODUZIONE

Al fine di affermare il proprio impegno verso il mercato e garantire un'efficace gestione della sicurezza delle informazioni, il Gruppo Atumtek ha deciso di definire ed implementare un sistema per la gestione per la sicurezza delle informazioni (in breve, SGSI) in conformità alla norma ISO/IEC 27001 e nel rispetto di quanto previsto dal Regolamento UE 2016/679 (di seguito GDPR).

Di fatto, l'adozione di un SGSI rappresenta una decisione strategica per l'organizzazione e vuole essere una dimostrazione della volontà di porsi formalmente in un'ottica di miglioramento continuo e di focalizzare le proprie attenzioni alla sicurezza dei servizi forniti ai clienti.

La presente politica, dunque, definisce gli obiettivi, i principi guida, i ruoli e le responsabilità necessari all'implementazione di suddetto sistema.

Va segnalato inoltre che, tutte le politiche e le procedure che compongono il framework documentale a supporto del SGSI referenziano e dipendono direttamente dalla presente politica. Tali documenti sono descritti all'interno del documento denominato "PR 01 - Procedura per la gestione della documentazione".

La presente politica sarà oggetto di riesame periodico e di eventuale successivo aggiornamento almeno annuale, al fine di garantire costantemente una corretta rappresentazione della situazione aziendale.

1.1 SCOPO DEL DOCUMENTO

Il presente documento ha lo scopo di definire i principi guida in materia di sicurezza delle informazioni, in conformità alla norma ISO/IEC 27001, da considerare per garantire il corretto funzionamento del SGSI di Atumtek. In quest'ottica ogni nuovo processo aziendale e sistema informativo che rientra nell'ambito di applicazione del SGSI deve essere progettato e realizzato in conformità alla presente politica.

Al momento dell'ultima revisione della presente Politica, il Gruppo Atumtek è una partnership commerciale, sprovvista di personalità giuridica. L'ambito su cui insiste il SGSI definito da Atumtek e che viene in questa prima fase sottoposto a certificazione è pertanto formalizzato come: "**Progettazione ed erogazione da parte della società Atum delle piattaforme applicative I2G, FEWFIne, FEWFINe Service Layer, attività di implementazione di "robot" e automazioni ("RPA") e servizi professionali di consulenza**.

Tutta la documentazione farà quindi riferimento al Gruppo Atumtek nonostante in una fase iniziale solo Atum Srl in qualità di capofila, sarà sottoposta a certificazione.

La definizione di questo campo di applicazione, dettagliato in termini di asset nell'ambito delle attività di gestione del rischio, inclusivo della strumentazione utilizzata, tiene in considerazione gli elementi definiti nei seguenti paragrafi.

1.2 CONTESTO

Come anticipato, Atumtek è una partnership commerciale, costituita nel 2022, tra tre società di professionisti esperti dell'Information Technology e della gestione di progetti IT per il settore assicurativo:

1) Intek, nata nel 2003;
2) Tecso – Tecnologia e Consulenza per Sistemi Organizzativi (in breve Tecso), nata nel 2009 e incorporata tramite fusione in Atum a fine 2024:
3) Atum Technologies & Solutions (in breve Atum), nata nel 2015.

Il Gruppo Atumtek si configura dunque come un brand commerciale che opera per supportare compagnie assicurative, banche, broker ed intermediari nella trasformazione digitale con soluzioni evolute di core business e gestione del cliente, offrendo loro soluzioni applicative a copertura dell'intero processo assicurativo.

L'acquisizione di Tecso da parte di Atum, iniziata nel 2020, si è conclusa attraverso la fusione per incorporazione a fine 2024. In previsione, nel prossimo futuro, anche l'ampliamento della partecipazione di Atum in Intek, iniziata nel 2021 con l'acquisizione del 30% del suo capitale sociale, per dare vita così ad un vero e proprio gruppo integrato di core insurance.

In tale contesto, Atumtek ha determinato i fattori interni ed esterni rilevanti, che influenzano (o possono influenzare) la sua capacità di raggiungere i risultati previsti dal SGSI, come descritti di seguito.

Fattori interni:

- Cultura dell'organizzazione: La cultura orientata alla sicurezza delle informazioni di Atumtek costituisce un elemento favorevole all'implementazione di un SGSI con il relativo insieme di politiche e procedure, che è in continua crescita.
- Politiche, obiettivi e strategie per raggiungerli: Politiche, procedure ed obiettivi rientrano nella cultura di Atumtek e il suo personale li sta seguendo. Gli obiettivi

di sicurezza delle informazioni sono noti e utilizzati e sono stati inclusi nella presente politica.

- Governance, struttura organizzativa, ruoli e responsabilità: È stato individuato il Responsabile della Sicurezza delle Informazioni così da garantire un livello di gestione adeguato e sono stati di conseguenza definiti formalmente ruoli e responsabilità, così come riportati anche nella presente politica.

- Standard, linee guida e modelli adottati dall'organizzazione: Atumtek ha stabilito una serie di norme di sicurezza delle informazioni che toccano diversi argomenti chiave.

- Relazioni contrattuali: I contratti con i fornitori e i prestatori di servizi sono controllati e vengono monitorati anche riguardo l'ambito della sicurezza delle informazioni.

- Processi e procedure: Le attività progettuali possono avere requisiti relativi alla sicurezza delle informazioni applicabili.

- Risorse e conoscenze: Sono allocate risorse specifiche relative alla sicurezza delle informazioni, come riportato nella presente politica.

- Sistemi informativi, flussi di informazioni e processi decisionali: I sistemi informativi sono ospitati presso Cloud Service Provider, il che permette di avvalersi di un ambiente sicuro per l'erogazione dei servizi.

- Audit precedenti o risultati di precedenti attività di risk assessment: La precedente attività di risk assessment sull'ambito descrive una situazione in crescita che necessita di perfezionamenti, in alcuni casi fondamentali per migliorare la postura di Atumtek in materia di sicurezza delle informazioni; è prevista una serie di azioni di trattamento coerenti.

- Dimensioni contenute dell'organizzazione: Le dimensioni contenute dell'organizzazione, con una relativa tendenza a non lavorare in modo strettamente proceduralizzato, abilitano da un lato una buona flessibilità mentre dall'altro possono essere limitanti in ottica di miglioramento continuo.

- Complessità organizzativa: Atumtek fin dal 2023 si è dotata di una struttura organizzativa e operativa trasversale alle società Atum Srl e Intek Srl che compongono il Gruppo. Tale struttura organizzativa opera in maniera trasversale su tutti gli asset di Gruppo e adotta in maniera uniforme e condivisa tutto il SGSI. A tale scopo e nell'ottica di formalizzare questo aspetto, è stato sottoscritto tra Atum Srl e Intek Srl un accordo di scambio di servizi in cui sono dettagliati l'oggetto dei servizi scambiati, le modalità dello scambio e i reciproci obblighi di riservatezza e di adeguamento al SGSI oggetto di certificazione.

Fattori esterni:

- Sociali e culturali: Non ci sono questioni sociali o culturali che possano influenzare l'istituzione di un SGSI e l'adozione e l'uso di procedure formalizzate.
- Politico, legale, normativo e regolamentare: Non ci sono questioni politiche, e legali, normative o regolamentari eccezionali che influenzano la sicurezza delle informazioni di Atumtek, a parte le leggi applicabili, elencate nel paragrafo 1.4 della presente politica, e i rapporti contrattuali con i fornitori. Atumtek, nello svolgimento dei servizi che eroga, può trovarsi nella condizione di dover sottostare alla normativa del settore assicurativo e ai regolamenti dell'istituto di vigilanza in tale ambito.
- Finanziari ed economici: La situazione finanziaria di Atumtek e le prospettive del settore sono in condizioni stabili-positive.
- Tecnologici: Le vulnerabilità del software e del firmware applicabili anche alle tecnologie di Atumtek e degli altri attori del mercato sono in aumento, influenzando tutti i tipi di asset ICT.
- Competitivi: I concorrenti e i criminali informatici stanno aumentando le loro capacità di sicurezza informatica, non interessando però attualmente Atumtek.
- Ambientali: Atumtek ha considerato gli impatti relativi al cambiamento climatico e, per l'attività svolta e per la tipologia di parti interessate, non sono emersi fattori significativi che possano influenzare lo scopo e la capacità per l'organizzazione di raggiungere gli obiettivi del proprio sistema di gestione.

Parti interessate e loro requisiti:

Nell'ambito del SGSI, le parti interessate e i relativi requisiti di sicurezza possono essere sintetizzati nella seguente tabella.

Parte interessata	Requisiti di sicurezza
Legislatore nazionale ed europeo	Normativa in ambito sicurezza delle informazioni
Autorità garante	Normativa in materia di protezione dei dati personali
Autorità di vigilanza	Normativa in materia di vigilanza sulle assicurazioni

Parte interessata	Requisiti di sicurezza
Soci e partner	Protezione delle informazioni aziendali di business e acquisite, con particolare attenzione ai dati personali
Clienti	Protezione delle informazioni aziendali acquisite, con particolare attenzione ai dati personali
Fornitori	Protezione delle informazioni aziendali inviate, con particolare attenzione ai dati personali
Dipendenti	Qualifiche del personale in ambito sicurezza delle informazioni

Tabella 1 - Parti interessate e relativi requisiti di sicurezza nell'ambito del SGSI

Considerando le modalità operative e la cultura aziendale, i professionisti (fornitori) sono trattati alla stregua del personale interno, a cui vengono pertanto applicate le stesse regole ed indicazioni di sicurezza. I fornitori, inoltre, sono legati dalle contromisure predisposte per la gestione dei rapporti con i fornitori e contenute nel modello MO 13 – Condizioni generali di fornitura, per quanto applicabili alle singole tipologie di fornitura.

La presente politica si applica a tutte le informazioni trattate da Atumtek all'interno del suo SGSI, indipendentemente dagli strumenti utilizzati per tali operazioni di trattamento e dai supporti su cui le informazioni sono memorizzate o trasmesse. Sono inoltre espressamente inclusi in questo contesto i fornitori che ne trattano le informazioni o che hanno comunque accesso ad esse.

1.3 LE INTERFACCE E LE INTERDIPENDENZE TRA LE ATTIVITÀ SVOLTE DIRETTAMENTE E INDIRETTAMENTE DALL'ORGANIZZAZIONE

La maggior parte delle attività di core business sono svolte direttamente, per quanto sono coinvolti una serie di soggetti esterni, solitamente nei panni di fornitori e con rapporti pertanto regolati da normali contratti di fornitura o dalle condizioni generali contenute nel modello "MO 13 – Condizioni generali di fornitura".

Attività	Soggetto	Interfaccia
Gestione dei progetti	Fornitori (collaboratori)	Direzione Aziendale
Gestione paghe e contributi	Fornitori (consulente del lavoro)	Amministrazione

Gestione della contabilità	Fornitori (commercialista)	Amministrazione
Cloud hosting	Fornitori (hosting providers)	Direzione Aziendale
Connettività e Internet	Fornitori (provider collegamenti fissi e mobile)	Amministrazione
Comunicazione e marketing	Fornitori (società di comunicazione)	Amministrazione
Sviluppo software	Partner (Intek S.r.l.) e Fornitori (collaboratori)	Direzione Aziendale

Tabella 2 - Interfacce e interdipendenze tra le attività svolte direttamente e indirettamente

1.4 RIFERIMENTI

Di seguito sono elencati le norme e i documenti di riferimento:

1) Norma tecnica ISO/IEC 27001
2) Norma tecnica ISO/IEC 27005
3) Regio Decreto 16 marzo 1942, n. 262 (Codice civile)
4) Legge 20 maggio 1970 n. 300 (Statuto dei Lavoratori)
5) Legge 10 dicembre 2014 n. 183 (Riforma del Jobs Act)
6) Decreto Legislativo 9 aprile 2008 n. 81 (Testo Unico sulla Sicurezza)
7) Regolamento generale per la protezione dei dati personali n. 2016/679 (GDPR)
8) Linee Guida n. 13 del 1° marzo 2007 (G.U. n. 58 del 10 marzo 2007)
9) Provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008 – Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema
10) Regolamento IVASS N. 38 del 3 Luglio 2018
11) "Decreto Legislativo 4 settembre 2024, n. 138" (NIS2)
12) PR 01 - Procedura per la gestione della documentazione

13) PR 02 - Procedura per la gestione del personale, uso accettabile degli strumenti e norme comportamentali

14) ATU - SOA 27002_2022

15) RE 05 - Censimento asset aziendali

16) Organigramma Gruppo Atumtek

17) Regolamento (UE) 2022/2554 (c.d. Digital Operational Resilience Act - DORA)

18) Atumtek MO 13 – Condizioni generali di fornitura

19) RE 17 - Registro assegnatari ruoli SGSI

1.5 ACRONIMI E DEFINIZIONI

Acronimo	Descrizione
SGSI	Sistema di Gestione per la Sicurezza delle Informazioni

2 PRINCIPI GUIDA E OBIETTIVI PER LA SICUREZZA

2.1 PRINCIPI GUIDA

La presente politica individua i seguenti principi guida da perseguire nell'implementazione del SGSI adottato da Atumtek:

ORIENTAMENTO AL CLIENTE

La fornitura di prodotti e servizi sicuri a tutti i Clienti è la missione ultima dell'azienda e deve essere sempre tenuta in massima considerazione nelle attività di tutti i giorni del personale.

RESPONSABILITÀ COLLETTIVA

La responsabilità per la sicurezza delle informazioni è un impegno collettivo e non un'attività demandata a specifiche risorse: ne consegue che tutti i dipendenti ed i collaboratori, senza nessuna esclusione, devono contribuire a salvaguardare la sicurezza aziendale.

GARANZIA PER TUTTO IL CICLO DI VITA

La sicurezza delle informazioni deve essere impostata e mantenuta durante tutto il ciclo di vita di un prodotto, servizio o informazione, ivi incluse acquisizione, pianificazione, creazione, archiviazione, accesso, modifica, manutenzione, trasmissione, salvataggio e distruzione. Questo concetto va applicato in modo specifico alla progettazione, nell'ottica di ottenere dei prodotti o servizi sicuri "by design" e già predisposti per essere operati al meglio "by default".

BILANCIAMENTO FRA RISCHI E CONTROMISURE

L'obiettivo delle contromisure non deve essere l'ottenimento di un irraggiungibile rischio nullo, bensì l'accurato e ponderato bilanciamento fra la valutazione dei rischi rilevati in un determinato ambito e il costo da sostenere per le relative contromisure. Quest'ultimo non deve superare quello dei rischi identificati.

SICUREZZA NELLA GESTIONE DEI PROGETTI

Per ogni progetto con impatti sulla sicurezza dell'informazione del servizio è prevista la conduzione di una analisi del rischio. Tale analisi viene effettuata dal proponente in conformità alla check list predisposta sul sistema di ticketing utilizzato dal Gruppo Atumtek che è emanazione diretta della check list per lo sviluppo sicuro denominata

"Atumtek – RE 09 Linee guida per lo sviluppo sicuro". Eventuali chiarimenti possono essere richiesti al Responsabile della Sicurezza delle Informazioni, l'analisi ha come scopo di rendere chiaro il rischio inerente ed il rischio ridotto conseguente all'implementazione dei controlli dell'Annex A della norma ISO/IEC 27001:2022. Il rischio residuo, a valle dell'analisi e delle misure di sicurezza proposte, deve essere accettato formalmente sia dal proponente che dal Responsabile del Progetto.

MIGLIORAMENTO CONTINUO

La realtà aziendale si evolve continuamente per rispondere alle esigenze di business o al progresso tecnologico e ogni processo o attività può e deve essere migliorato in modo costante nel tempo. Combinando queste due considerazioni ne consegue che l'approccio da seguire deve essere ricondotto a un processo circolare, le cui fasi principali sono:

- Pianificazione di un'azione, miglioramento o soluzione;
- Esecuzione di tutte le attività legate all'azione;
- Valutazione dei risultati ottenuti e verifica di raggiungimento degli obiettivi;
- Controllo e misurazione dei risultati, finalizzato ad individuare nuovi punti di miglioramento e a verificare la bontà delle azioni intraprese.

La circolarità dell'approccio si realizza nel ritorno dall'ultimo punto citato al primo, contribuendo a creare un circolo virtuoso orientato al miglioramento continuo.

NEED-TO-KNOW E PRIVILEGI MINIMI

L'accesso alle informazioni aziendali deve essere autorizzato in modo da consentire la consultazione, la modifica, la trasmissione e la distribuzione delle informazioni ai soli soggetti che ne necessitano per lo svolgimento delle proprie mansioni lavorative, limitatamente all'intervallo temporale richiesto. Di conseguenza, i privilegi di accesso assegnati devono essere limitati al minimo indispensabile per svolgere le relative mansioni.

DIFESA MULTILIVELLO

Le minacce e le vulnerabilità possono insistere su diversi livelli di un'infrastruttura tecnologica, pertanto, all'atto del disegno e dell'implementazione delle misure di sicurezza deve essere sempre rispettato il principio della difesa multilivello (defense in depth), prevedendo differenti tipologie di protezione per ciascun livello architetturale.

SEPARAZIONE DEI RUOLI

L'assolvimento di operazioni critiche per la sicurezza delle informazioni o dei sistemi informativi a supporto deve sempre rispettare il principio della separazione dei ruoli (separation of duties), ovvero assicurando che un soggetto non si trovi mai nelle condizioni di completare un'operazione critica in completa autonomia. Per operazioni particolarmente critiche va previsto altresì il ricorso agli analoghi principi di segreto condiviso (split knowledge) e doppio controllo (dual control).

INEFFICACIA DELLA NON DIVULGAZIONE

L'adozione di soluzioni aperte, documentate e verificabili è sempre preferibile a quella di soluzioni proprietarie e segrete e un metodo di protezione non deve essere considerato tale solo perché il suo uso o le sue caratteristiche non sono note.

DOCUMENTAZIONE E COLLABORAZIONE

La scelta delle misure di sicurezza deve prevedere un processo decisionale documentato che dimostri la corretta implementazione dei requisiti di sicurezza.

2.2 OBIETTIVI

La presente politica individua gli obiettivi del SGSI, nell'ambito della sicurezza delle informazioni, adottati da Atumtek in:

- minimizzazione del numero degli incidenti di sicurezza delle informazioni;
- riduzione del livello di rischio determinato dal processo di risk assessment;
- ottenimento e successivo mantenimento della certificazione ISO/IEC 27001.

3 RUOLI E RESPONSABILITÀ NEL SGSI

3.1 ASSETTO ORGANIZZATIVO DI ATUMTEK

La struttura organizzativa di Atumtek e le principali unità organizzative in cui essa è articolata sono definite dal documento "Organigramma SGSI Gruppo Atumtek". Tramite documento specifico di nomina vengono esplicitati le responsabilità e i compiti di ciascun componente. L'elenco dei componenti è riportato nell'apposito registro "RE 17 - Registro assegnatari ruoli SGSI".

I soggetti chiamati a ricoprire le diverse posizioni in ambito aziendale rispondono, nell'ambito delle proprie attribuzioni, per gli atti alla cui predisposizione ed esecuzione abbiano provveduto o collaborato e per l'omissione di attività alle quali sono tenuti, per ordine di direzione o per altre disposizioni interne, secondo il procedimento disciplinare dettagliato nel documento "PR 02 - Procedura per la gestione del personale, uso accettabile degli strumenti e norme comportamentali".

Nei paragrafi a seguire si definiscono i ruoli chiave definiti da Atumtek rispetto al Sistema di Gestione per la Sicurezza delle Informazioni e le relative responsabilità in ambito SGSI.

La definizione di ruoli e responsabilità è gestita seguendo il principio della separazione dei compiti (segregation of duties), prevedendo che compiti e aree di responsabilità in conflitto tra loro vengano separati.

Nello specifico, considerata la presenza diffusa all'interno dell'azienda di competenze tecnico-informatiche in ragione delle attività di core business, la Direzione Aziendale ha ritenuto opportuno suddividere i compiti e le responsabilità tra il Responsabile per la Sicurezza delle Informazioni e il Responsabile IT identificando nel primo una figura di compliance e assegnandogli maggiori responsabilità nell'ambito della governance del SGSI e della sua conformità alle norme e alle certificazioni raggiunte; mentre il secondo viene identificato come una figura di direzione e coordinamento per l'applicazione sul piano tecnico delle decisioni strategiche aziendali in tema di sicurezza con specifico riguardo alla sicurezza IT.

La presente politica, approvata dalla Direzione Aziendale, rappresenta l'assunzione di impegno da parte della direzione stessa, in ambito di sicurezza delle informazioni. La Direzione Aziendale garantisce in questo modo il proprio impegno nel:

- soddisfare i requisiti di sicurezza delle informazioni applicabili nel contesto del SGSI;
- promuovere il miglioramento continuo del SGSI.

3.2 DIREZIONE AZIENDALE

La Direzione Aziendale è la massima autorità all'interno della SGSI ed ha la titolarità di tutte le informazioni trattate da essa. Le sue responsabilità in tema di SGSI sono le seguenti:

- approvare la politica e gli obiettivi per la sicurezza delle informazioni in modo che siano compatibili con gli indirizzi strategici e tattici dell'organizzazione e nell'ottica di miglioramento continuo del SGSI;
- approvare l'organigramma del SGSI, definendo ruoli e responsabilità, ed assicurare la disponibilità del personale al SGSI;
- approvare le azioni di trattamento del rischio;
- approvare le risorse allocate in materia di sicurezza delle informazioni;
- approvare il sistema di gestione delle informazioni aziendali;
- approvare la predisposizione dei dispositivi di lavoro e delle utenze per il nuovo personale in ingresso;
- approvare il processo di apertura/chiusura delle utenze per il personale in entrata/uscita;
- approvare e gestire, con il supporto dei relativi responsabili, il budget a disposizione in materia di sicurezza delle informazioni.

Di seguito sono definiti i compiti della Direzione Aziendale:

- gestire le comunicazioni verso l'esterno relative alla sicurezza delle informazioni;
- supervisionare i documenti propri del SGSI (politiche, procedure) redatti per soddisfare i requisiti delle norme applicabili, definendo eventuali modifiche;
- analizzare i risultati degli audit interni ed esterni ed i documenti che evidenziano l'efficacia o le carenze del SGSI, ad esempio i dati degli indici di misurazione, azioni di miglioramento e correttive;
- analizzare l'efficacia delle azioni intraprese, apportando e deliberando le modifiche che ritiene necessarie;
- gestire il processo di selezione del personale;
- definire le necessità formative in materia di sicurezza delle informazioni;

- verificare le competenze e le responsabilità delle figure aziendali;
- nominare il Responsabile della Sicurezza delle Informazioni, coordinando e verificando anche tramite audit interni le attività assegnategli;
- comunicare al Responsabile della Sicurezza delle Informazioni l'avvio del processo di apertura/chiusura delle utenze per il personale in entrata/uscita;
- approvare le implementazioni proposte in ordine alla compliance aziendale alla normativa vigente in ambito privacy;
- gestire il processo di gestione e monitoraggio dei fornitori e degli approvvigionamenti;
- comunicare al Responsabile della Sicurezza delle Informazioni le necessarie informazioni relative alla gestione dei dispositivi di lavoro, delle utenze e dei profili per il nuovo personale;
- approvare le richieste di accesso a sistemi/applicativi di Atumtek non previste dal profilo standard;
- contattare e comunicare con i fornitori eventualmente colpiti dall'avvenimento di un incidente IT e di sicurezza delle informazioni nell'Organizzazione;
- supervisionare l'erogazione dei servizi di Atumtek per l'ambito della sicurezza delle informazioni.

La Direzione Aziendale nomina il Referente di Direzione che è la diretta emanazione della Direzione Aziendale all'interno del Gruppo di Lavoro che si occupa della gestione e del mantenimento del SGSI e svolge l'attività di aggiornamento e condivisione all'interno della Direzione Aziendale delle esigenze per il mantenimento e l'implementazione del SGSI.

3.3 Responsabile della Sicurezza delle Informazioni

Il Responsabile della Sicurezza delle informazioni è il responsabile di massimo livello per la sicurezza delle informazioni e risponde direttamente alla Direzione Aziendale su tale tematica.

Le sue responsabilità in ambito SGSI sono le seguenti:

- assolvere il ruolo di punto di riferimento aziendale in materia di sicurezza delle informazioni;

- garantire un corretto e costante presidio della sicurezza delle informazioni relativamente a tutte le attività svolte da Atumtek;
- supportare la Direzione Aziendale nella gestione delle risorse per la sicurezza delle informazioni;
- coordinare il personale dell'azienda con responsabilità in materia di sicurezza delle informazioni;
- mantenere la conformità a leggi, regolamenti, contratti e norme tecniche applicabili per la loro componente di sicurezza delle informazioni;
- assicurare e controllare la rilevazione, la risoluzione e consuntivazione degli incidenti relativi alla sicurezza delle informazioni;
- gestire le comunicazioni in materia di sicurezza delle informazioni interne ad Atumtek;
- gestire i cambiamenti al SGSI.

Di seguito sono definiti i compiti:

- organizzare le responsabilità operative relative alla sicurezza delle informazioni;
- proporre la strategia per la gestione della sicurezza delle informazioni alla Direzione Aziendale;
- controllare periodicamente il livello complessivo di sicurezza delle informazioni aziendali;
- informare periodicamente la Direzione Aziendale sullo stato della sicurezza delle informazioni e sulle performance del SGSI;
- garantire la conformità del sistema di gestione alle norme applicabili;
- supportare Atumtek nell'individuazione delle misure di sicurezza delle informazioni adeguate, ed indirizzare la sicurezza delle informazioni nella gestione dei progetti aziendali;
- presentare la relazione inerente ai rischi alla Direzione Aziendale;
- assicurare l'esecuzione del piano di trattamento del rischio;
- assicurare e controllare la rilevazione, la risoluzione e consuntivazione degli incidenti relativi alla sicurezza delle informazioni;

- presiedere la redazione e l'aggiornamento delle policy e delle procedure per la sicurezza delle informazioni;
- supportare la Direzione Aziendale nella gestione delle risorse allocate per la sicurezza delle informazioni;
- approvare le procedure per l'accesso e la profilazione degli utenti sui sistemi/applicazioni;
- supportare il management nel processo di gestione dei fornitori e degli approvvigionamenti;
- supportare la Direzione Aziendale nella verifica della sicurezza delle informazioni nella progettazione dei servizi erogati dall'Organizzazione.

3.4 RESPONSABILE IT

È responsabilità del Responsabile IT svolgere le proprie attività nell'osservanza e nell'applicazione pratica di quanto stabilito nei documenti dei processi del SGSI.

In particolare, i suoi principali compiti in ambito SGSI sono:

- gestire la continuità operativa di Atumtek, adottando i piani e le procedure ad essa dedicati;
- assicurare la configurazione sicura delle postazioni di lavoro aziendali, il funzionamento delle misure tecniche di sicurezza e degli account aziendali:
- assicurare e controllare la rilevazione, la risoluzione e consuntivazione degli incidenti IT;
- gestire gli inventari e le configurazioni di sicurezza di default dei dispositivi aziendali;
- disciplinare la gestione e le modalità di raccolta e conservazione dei log dei sistemi;
- verificare periodicamente i software installati sui dispositivi aziendali;
- analizzare periodicamente i log per il monitoraggio dei sistemi informatici;
- abilitare le utenze per il personale in entrata su richiesta dell'organizzazione;
- gestire i cambiamenti ai sistemi informativi in relazione alle esigenze dell'organizzazione;

- individuare e valutare le nuove patch di sicurezza in base ai bollettini emessi dai fornitori oppure in base agli strumenti messi a disposizione dall'organizzazione;
- effettuare la disabilitazione delle utenze per il personale in uscita su richiesta dell'organizzazione;
- garantire l'applicazione dei principi di sicurezza propri del SGSI nell'ambito della gestione delle change;
- fare in modo che vengano predisposte e rese funzionanti le copie di sicurezza (operazioni di backup e recovery) dei dati e delle applicazioni, quando necessario tramite gli strumenti messi a disposizione dall'organizzazione.

3.5 Responsabile Privacy

È responsabilità del Responsabile Privacy svolgere le proprie attività nell'osservanza e nell'applicazione pratica di quanto stabilito nei documenti dei processi del SGSI e nei documenti relativi ai processi in ambito privacy. In particolare, i suoi principali compiti sono:

- manutenere e aggiornare periodicamente la documentazione aziendale in materia di trattamento dati personali (nello specifico il documento "RE - 06 Registro delle attività di trattamento del titolare");
- informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dalle procedure GDPR, nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;
- sorvegliare l'osservanza del regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
- fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne il rispetto ai sensi dell'articolo 35 del GDPR nello svolgimento delle attività;
- cooperare con l'autorità di controllo;
- fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36 del GDPR, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione;

- verificare periodicamente le attività svolte degli amministratori di sistema, in modo da controllare la loro rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali, previste dalle norme vigenti e dalle procedure aziendali;

- supportare il Responsabile IT e/o il Responsabile per la Sicurezza delle Informazioni a gestire le azioni di reazione ad incidenti IT e/o incidenti relativi alla sicurezza delle informazioni, nel caso in cui questi abbiano un impatto sulla protezione dei dati personali.

3.6 ALTRI ATTORI

Altri attori che possono avere un ruolo di rilievo in materia di sicurezza delle informazioni sono i seguenti:

3.6.1 Amministratori di sistema

È responsabilità degli amministratori di sistema, istruiti e formati per competenze e che hanno ricevuto apposita nomina formalizzata nel documento di nomina ad amministratori di sistema, svolgere le proprie attività nell'osservanza e nell'applicazione pratica di quanto stabilito nei documenti dei processi del SGSI. In particolare, specificatamente e limitatamente al contesto in cui operano, i loro compiti sono:

- custodire le credenziali per la gestione dei sistemi IT predisposti dall'organizzazione;

- predisporre e rendere funzionali le copie di sicurezza (operazioni di backup e recovery) dei dati, dei sistemi e delle applicazioni rispettando le tempistiche definite dall'organizzazione;

- amministra e configura i programmi antivirus, firewall ed altri strumenti software o hardware messi a disposizione dall'organizzazione al fine di garantire adeguate misure di sicurezza nel rispetto di quanto previsto dalla disciplina in materia di protezione dei dati personali;

- provvedere alla cancellazione logica dei dati dai sistemi e dai supporti di memorizzazione in base alle modalità ed alle tempistiche definite dall'organizzazione.

3.6.2 Tutto il personale

È responsabilità di ogni risorsa del personale, istruita e formata per competenze, essere consapevole delle politiche e delle procedure del SGSI e del proprio contributo

all'efficacia dello stesso, svolgendo le proprie attività nell'osservanza e nell'applicazione pratica di quanto stabilito nei documenti dei processi del SGSI.

Compito di ogni collaboratore coinvolto nell'erogazione dei processi aziendali è quello di garantire un adeguato livello di protezione delle informazioni e dei dati aziendali, partecipando direttamente al mantenimento dei livelli di sicurezza previsti in termini di riservatezza, integrità e disponibilità. Tutti i soggetti hanno ruolo esecutivo sul processo indicato.