ISO27001:2022
Information Security Policy

Società di riferimento	**APPLIED**
Perimetro di validità	Gruppo Applied
Ambito documento	ISMS
Codificazione	APPL-ISMS-PL-001
Nome esteso documento	APPL-ISMS-PL-001-Information Security Policy-v01
Documento:	Information Security Policy
Versione	1 del 02/05/2024
Lingua	Italiano
Approvatore	Head of P & S Committee
Autore	Cyber Security & Compliance Manager
Data di approvazione	02/05/2024

TABELLA REVISIONI

Versione	Data	Autore	Note
0.1	27/03/2024	Cyber Security & Compliance Manager	Creazione del documento
0.1	02/05/2024	Head of P&S Committee	Approvazione del documento

1. INTRODUZIONE

L'insieme delle strutture organizzative, delle politiche, delle procedure, dei controlli e delle tecnologie progettate per proteggere le risorse informatiche e più generalmente il patrimonio informativo aziendale è comunemente inteso come un Sistema di Gestione della Sicurezza delle Informazioni (SGSI).

Lo standard **ISO 27001:2022** (*il cui nome completo ora è ISO/IEC 27001:2022/Amd 1:2024 con l'introduzione dei requisiti relativi il Climate Change*) è uno standard di riferimento internazionale per la Sicurezza delle Informazioni, che fornisce i requisiti per la costituzione di un Sistema di Gestione della Sicurezza delle Informazioni.

Il termine Information Security in questo documento è inteso come un insieme di misure atte a garantire i tre principi fondamentali della sicurezza:

- **Riservatezza**: il rischio che l'accesso all'informazione (inteso come dati o programmi) sia assegnato rifiutato in modo inappropriato;
- **Integrità**: il rischio che le informazioni siano modificate o cancellate, accidentalmente o intenzionalmente, da parte di coloro i quali non hanno la qualifica per farlo;
- **Disponibilità**: il rischio che le informazioni non siano disponibili quando necessario.

La protezione delle informazioni deve, inoltre, seguire i **7 livelli Cyber**:

Livello	Goal
Physical Security	Mettere in sicurezza l'accesso all'infrastruttura e agli hardware
Network Security	Proteggere l'infrastruttura network e flusso dei dati
Perimeter Security	Controllare l'accesso al network attraverso routers e gateways
Endpoint Security	Proteggere i dispositivi connessi al network
Application Security	Mettere in sicurezza il software e le applicazioni running nel network
Data Security	Mettere in sicurezza la conservazione e trasmissione dei dati nel network
User Security	Educare gli utenti verso le best practices della cyber security

2. DEFINIZIONI

Need to know

Principio per cui l'utente accede soltanto ai dati strettamente necessari per eseguire le attività di propria competenza (i.e. secondo le mansioni assegnate aziendalmente).

Rischio

Il rischio è un evento che potrebbe portare un impatto (negativo) sul raggiungimento degli obiettivi di business. L'impatto di questo rischio è proporzionale al valore della perdita nel contesto del business dell'azienda e dipendente dalla frequenza stimata con la quale la perdita di valore potrebbe materializzarsi.

Segregation of Duty

Principio che mira a separare le attività in modo da evitare la concentrazione di più attività critiche nelle mani della stessa persona / funzione.

SGSI (Sistema di Gestione per la Sicurezza delle Informazioni) o ISMS (Information Security Management System)

Insieme delle politiche, procedure, linee guida, risorse e attività associate, gestite da un'organizzazione al fine di proteggere i propri asset informativi. Un SGSI è un approccio sistematico per stabilire, attuare, condurre, monitorare, riesaminare, mantenere e migliorare la sicurezza delle informazioni di un'organizzazione per raggiungere gli obiettivi di business.

Sicurezza delle informazioni

Conservazione della riservatezza, dell'integrità e della disponibilità delle informazioni; inoltre, possono essere coinvolte altre proprietà quali l'autenticità, la responsabilità, il non ripudio e l'affidabilità

Confidenzialità

Proprietà per cui l'informazione non è resa disponibile o rivelata a individui, entità o processi non autorizzati.

Contesto esterno

Ambiente esterno nel quale l'organizzazione cerca di conseguire i propri obiettivi.

Contesto interno

Ambiente interno nel quale l'organizzazione cerca di conseguire i propri obiettivi.

Disponibilità

Proprietà di essere accessibile e utilizzabile su richiesta di un'entità autorizzata.

Integrità

Proprietà relativa alla salvaguardia dell'accuratezza e della completezza dei beni.

Parte interessata

Persona o organizzazione che può influenzare o essere influenzata da una decisione o un'attività.

Requisito

Proprietà per cui l'informazione non è resa disponibile o rivelata a individui, entità o processi non autorizzati.

3. SCOPO

L'obiettivo di questo documento è stabilire la direzione generale e strategica da perseguire al fine di prevenire i rischi connessi al trattamento delle informazioni e di proteggere il patrimonio informativo aziendale e delle Legal Entity.

Nello specifico, la presente politica in materia di sicurezza delle informazioni è stata definita considerando le best practice in materia di sicurezza delle Informazioni, con particolare riferimento ai seguenti standard:

- ISO/IEC 27001:2022/Amd 1:2024 Information Technology – Information Security Management Systems – Requirements;
- ISO 27002:2022 Information Technology – Code of Practice for Information Security Controls.

4. AMBITO DI APPLICAZIONE

Il presente documento deve essere considerato fonte di riferimento sulle tematiche in oggetto da tutte le realtà del Gruppo Applied e deve essere applicato in ciascuna aziende in ottemperanza alla policy centrale. La policy si applica a tutti gli utenti Applied inclusi i dipendenti, il personale di provider esterni di servizi, e altre tipologie di collaboratori. Il personale del Gruppo adotterà misure al fine di garantire il rispetto della presente policy.

La presente annulla e sostituisce tutte le eventuali precedenti procedure emesse in materia e ha validità immediata.

5. MODELLO DI GESTIONE DELLA SICUREZZA DEL GRUPPO APPLIED

Applied si è prefissata una serie di "Obiettivi Strategici di Sicurezza", che hanno lo scopo di garantire:

- Il raggiungimento delle strategie aziendali di sicurezza
- La confidenzialità, integrità, disponibilità del patrimonio informativo.

Gli Obiettivi Strategici sono declinati in Obiettivi del SGSI di maggior dettaglio e dal contenuto più tecnico, descritti all'interno del presente documento.

Gli Obiettivi SGSI, come da norma internazionale ISO27001:2022, comprendono tutte le attività e controlli che permettono la creazione e monitoraggio continuo di un sistema di gestione di sicurezza delle informazioni. L'output delle procedure di misurazione degli Obiettivi Strategici e degli Obiettivi SGSI producono un elenco di misure di sicurezza necessarie da implementare per perseguire gli obiettivi sopracitati.

In conclusione, al fine di garantire adeguati livelli di sicurezza connessi ai sopra citati principi, le società del Gruppo Applied si prefiggono il raggiungimento dei seguenti obiettivi, distinti nelle due categorie di seguito descritte:

- ***Obiettivi Strategici di Sicurezza***, finalizzati al raggiungimento degli obiettivi di business strategici di sicurezza nel rispetto dei principi di confidenzialità, integrità e disponibilità del patrimonio informativo.
- ***Obiettivi del SGSI,*** finalizzati alla realizzazione, manutenzione e miglioramento continuo del sistema di gestione, nonché strumentali al raggiungimento degli "Obiettivi Strategici di Sicurezza".

6. OBIETTIVI STRATEGICI DI SICUREZZA

Al fine di assicurare il completo allineamento tra la propria strategia di business e la tutela del patrimonio informativo aziendale, Applied ha definito degli obiettivi specifici in materia di Strategia di Sicurezza.

Il processo di Risk Management assicura la gestione dei rischi che minacciano il raggiungimento degli obiettivi stessi.

6.1 Strategia aziendale rispetto alle Normative vigenti

Garantire la conformità alle specifiche norme vigenti in materia di sicurezza, privacy, confidenzialità, trattamento e protezione dei dati personali, monitorando eventuali variazioni delle norme stesse.

6.2 Innovazione Tecnologica

Garantire livelli di protezione adeguati delle informazioni conformi agli obiettivi del servizio, anche a fronte di innovazioni e progressi tecnologici e dei rischi, anche cyber, ad essi associati tra cui il Data Loss, Data Breach.

6.3 Tutela dei dati (dipendenti, clienti, fornitori, third parties)

Garantire la sicurezza dei sistemi, l'integrità della documentazione archiviata e la disponibilità del servizio ai dipendenti e third parties. Salvaguardare le informazioni confidenziali dei clienti da potenziali rischi quali accesso non autorizzato, Data Loss e Data Breach. Assicurare il rispetto delle clausole contrattuali di sicurezza richieste dal cliente.

6.4 Obiettivi e priorità di Applied

Garantire la conformità agli obiettivi strategici e priorità del business anche in materia di tutela dei dati personali e confidenziali.

6.5 Sistemi e Tecnologie

Garantire l'efficienza della tecnologia a supporto delle attività operative, al fine di limitare gli impatti sulla profittabilità del Gruppo, in modo tale da prevenire un disallineamento tra le strategie IT e le strategie business.

6.6 Outsourcer e Fornitori

Garantire il controllo dei livelli di servizio erogati dai fornitori ed il rispetto delle clausole di sicurezza definite negli accordi di servizio (Service Level Agreement – SLA).

6.7 Risorse Umane

Garantire la capacità di assumere e mantenere personale sufficientemente qualificato e competente al fine di limitare la possibilità che si verifichino incidenti di sicurezza a seguito di errori o accessi non autorizzati da parte del personale che eroga i servizi.

6.8 Garantire la Continuità del Business

Garantire la continuità e la disponibilità del servizio in seguito a disastri o malfunzionamenti.

7. OBIETTIVI DEL SISTEMA DI GESTIONE DI SICUREZZA DELLE INFORMAZIONI

I requisiti e i principi generali di sicurezza sono contestualizzati all'interno dell'organizzazione tramite obiettivi di carattere operativo e regolamentare finalizzati a supportare la realizzazione e il mantenimento del SGSI.

In linea con i principi stabiliti all'interno della norma ISO27001, il SGSI deve conseguire le seguenti finalità principali:

- Security Policies
- User Responsibilities
- Organization of Security
- Human Resource Security
- Privacy
- Asset Management
- Access Control
- Cryptography
- Physical & Environmental Security
- Operations Security
- Communications Security
- System acquisition, development and maintenance
- Supplier relationships
- Information security incident management
- Business continuity management
- Compliance

Di seguito vengono descritte in dettaglio i domini di sicurezza sopraelencati:

7.1 Security Policies

Fornire direttive e supporto per le tematiche di sicurezza in linea con i requisiti di business, leggi e regolamenti. Sono formalizzate delle policy di dettaglio su temi specifici, diffuse all'intera platea aziendale e disponibili all'interno dell'ISMS sullo SharePoint aziendale.

7.2 User Responsibilities

Garantire che i dipendenti del Gruppo Applied, acquisiscano piena consapevolezza del ruolo centrale che la l'utente stesso nei confronti della tutela dei dati e segnalazione di circostanze sospette. La formazione che viene erogata è diretta in questo senso, nel diffondere delle "buone regole di comportamento". Alcune regole condivise all'interno del corso "Fondamenti di Cyber Security", corso obbligatorio per tutti i dipendenti:

- ***Custodire in modo corretto i dispositivi aziendali*** (custodire i dispositivi aziendali e bloccare lo schermo del computer quando ci si allontana dalla propria postazione di lavoro)
- ***Usare in modo corretto le risorse aziendali*** (non rimuovere, installare o modificare alcuna componente Hardware o Software se non preventivamente autorizzati)
- ***Mantenere la postazione di lavoro "pulita"*** (prestare attenzione a fogli, schemi, appunti o qualsiasi altro documento cartaceo dal quale sia possibile dedurre anche indirettamente informazioni a carattere personale o riservate di Applied)
- ***Proteggere la componente segreta della credenziali personali*** (custodire password/pin con massima diligenza avendo cura di non comunicarle ad altri. Avere cura di cambiare la password in caso di sospetta violazione)
- ***Usare in modo corretto Internet*** (non effettuare download di software gratuiti e non inviare informazioni aziendali riservate se non espressamente autorizzati)
- ***Usare in modo corretto la Posta Elettronica*** (utilizzare la posta aziendale solo per finalità lavorative e segnalare tramite il canale dedicato eventuali e-mail sospette)
- ***Compressione e cifratura dei file*** (7-zip è lo strumento di compressione e cifratura suggerito da Applied. Deve essere utilizzato per invio di dati personali, inviando la password per altra via)

- ***Segnalare tempestivamente di incidenti di sicurezza*** (segnalare senza ritardo eventuali casi di violazione o di sospetta violazione della sicurezza)
- ***Fare attenzione alla Tipologia di Informazioni*** (utilizzare le label implementate da Applied per distinguere il livello di confidenzialità delle informazioni: Segreto, Confidenziale, Ristretto, Pubblico)

7.3 Organization of Security

Stabilire un Management Framework per avviare e mantenere il sistema di gestione della sicurezza con una adeguata allocazione di risorse e responsabilità, nonché garantire la sicurezza del telelavoro e nell'uso dei dispositivi mobili.

7.4 Human resource security

Assicurare che il Management e il personale, partner e dipendenti, e principali fornitori comprendano le loro responsabilità, siano consapevoli e adempiano a pieno alle loro responsabilità in ambito security, e che gli interessi di Applied siano tutelati nel processo di selezione, avvio, modifica o cessazione del rapporto di lavoro.

In caso di comportamenti scorretti o che violano le policy in materia di Information Security, i dipendenti saranno soggetti a richiami/provvedimenti disciplinari secondo il CCNL di riferimento.

7.5 Training e formazione continua

Applied garantisce una formazione su temi Cyber Security, Data Classification e formazione specifica. Sono previste campagne di phishing e pillole formative con l'obiettivo di aumentare l'awareness e sensibilizzazione da parte di tutti i suoi dipendenti.

7.6 Privacy

Assicurare che Applied abbia una corretta gestione, e periodico aggiornamento, dei processi e procedure per garantire la protezione dei dati personali che circolano in azienda. In particolare con riferimento ai dati dei dipendenti, collaboratori, fornitori e clienti. Le società del Gruppo detengono un Registro dei

Trattamenti (utilizzando la piattaforma Utopia), ove sono aggiornati i trattamenti effettuati, sia in riferimento al Registro come Titolari del Trattamento che come Responsabile del Trattamento verso i propri clienti.

7.7 Data Classification & Protection Model

Assicurare che il personale di Applied sappia classificare nel modo più opportuno le informazioni gestite e applicare ad ogni livello inviduato (Segreto, Confidenziale, Ristretto e Pubblico) le misure di sicurezza più opportune.

7.8 Asset management

Individuare le risorse del Gruppo, definire adeguate responsabilità sulla protezione, sviluppare controlli di sicurezza commisurati all'importanza dell'asset e impedire la divulgazione non autorizzata, modifica, rimozione o distruzione delle informazioni memorizzate su supporti.
Rientrano in tal senso anche le misure di sicurezza relative alla gestione dei dispositivi mobili (implementazione MAM – Mobile Application Management presente in tutte le applicazioni aziendali accedute tramite account Applied sul dispositivo, aziendale o personale, Android e i OS).

7.9 Access control

Limitare l'accesso alle informazioni ed ai sistemi in accordo con il principio di minimo privilegio, garantire l'accesso degli utenti autorizzati e prevenire l'accesso non autorizzato a sistemi e servizi, rendere gli utenti responsabili per salvaguardare le loro informazioni di autenticazione (Username, Password, eventuali token o secure code) e impedire l'accesso non autorizzato a sistemi e applicazioni.

7.10 Cryptography

Garantire un uso corretto ed efficace della crittografia per proteggere la riservatezza, l'autenticità e / o l'integrità delle informazioni.

7.11 Physical & environmental security

Impedire l'accesso fisico non autorizzato, danni e interferenze alle informazione ed ai sistemi di elaborazione delle informazioni, così come altre strutture, e impedire accessi non autorizzati, perdita, danneggiamento, furto o la compromissione di asset aziendali e l'interruzione delle operazioni.

7.12 Operations security

Garantire il corretto e sicuro funzionamento dei sistemi di elaborazione delle informazioni, la protezione contro malware e perdita di dati e prevenire lo sfruttamento delle vulnerabilità tecniche da parte di malintenzionati.
Garantire controlli adeguanti per registrare gli eventi e fornire le evidenze, garantire l'integrità dei sistemi operativi e ridurre al minimo l'impatto delle attività di controllo sui sistemi stessi.

7.13 Communications security

Garantire la protezione delle informazioni nelle reti di telecomunicazione e mantenere la sicurezza delle informazioni trasferite internamente e con le organizzazioni esterne.

7.14 System acquisition, development and maintenance

Garantire che la sicurezza delle informazioni e la protezione dei dati siano parte integrante del ciclo di vita dei sistemi informativi, a partire dal disegno, testing e implementazione di sistemi e / o servizi.

7.15 Supplier relationships

Garantire la protezione degli asset accessibili dai principali fornitori, mantenere il livello di sicurezza delle informazioni concordato e fornire servizi in linea con gli accordi stabiliti.

7.16 Information security incident management

Garantire un approccio coerente ed efficace per la gestione dei security incident (ad esempio, rilevamento, contenimento e risoluzione), e garantire la comunicazione e condivisione degli eventi e delle vulnerabilità di sicurezza.

7.17 Business continuity management

Implementare i controlli per il crisis management, business continuity e disaster recovery, garantire che la continuità della sicurezza delle informazioni sia incorporata nei sistemi di gestione della business continuity, allo stesso modo prevedere che la disponibilità delle facilities a supporto delle elaborazioni sia garantita tramite sistemi ridondati.

7.18 Compliance

Impedire violazioni ai requisiti normativi, statutari, regolamentari o contrattuali relativi alla sicurezza e garantire che la sicurezza sia implementata e gestita in accordo con le politiche e le procedure applicabili.

7.19 Climate Change

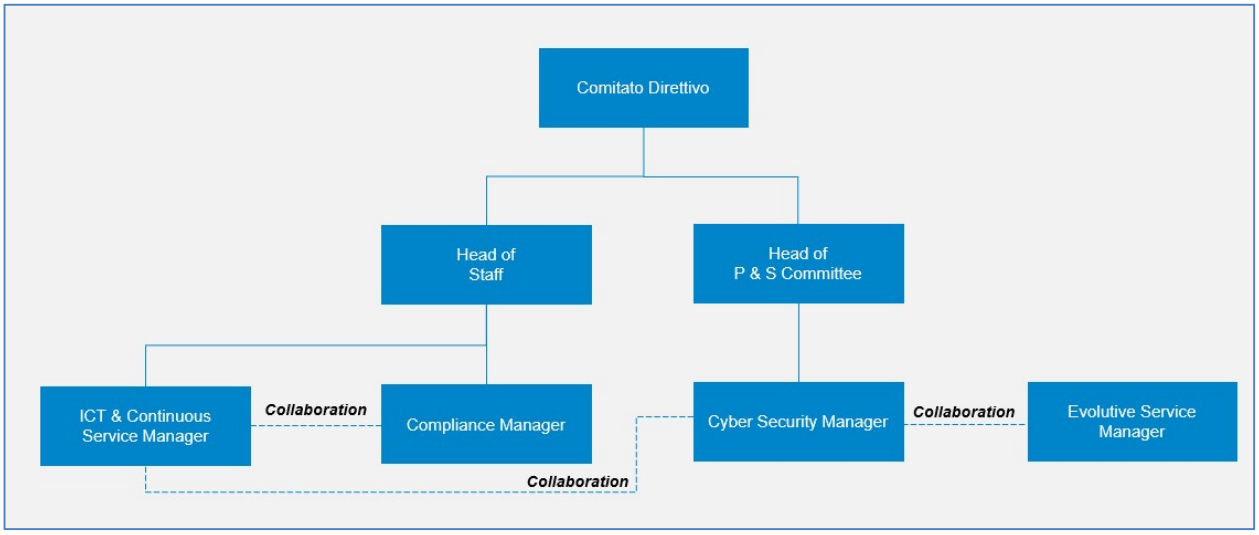
Il tema del cambiamento climatico è di stretta attualità e impatta anche sui sistemi di gestione della sicurezza delle informazioni. Applied ha determinato che il cambiamento climatico è una questione rilevante ed ha messo in atto delle misure apposite.

8. RUOLI E RESPONSABILITÀ

La gestione della Sicurezza delle Informazioni deve essere parte integrante degli obiettivi di business e deve coinvolgere le necessarie risorse ad ogni livello organizzativo. E' infatti imprescindibile che la sicurezza delle informazioni sia supportata, sia visibilmente che materialmente, dal senior management. Sussistono aspetti specifici del sistema di gestione in cui l'alta direzione dimostra sia leadership che impegno. Questi includono ma non sono limitati a:

- Responsabilità per l'efficacia dell'ISMS;
- Garantire che la politica e gli obiettivi siano stabiliti e siano compatibili con il contesto e la direzione strategica dell'organizzazione;
- Garantire che l'integrazione dell'ISMS sia incorporata nei processi aziendali;
- Promuovere l'uso dell'approccio per processi e della strategia basata sul rischio;
- Garantire che siano disponibili risorse adeguate;
- Garantire che l'ISMS raggiunga i risultati previsti;
- Coinvolgere, dirigere e sostenere le persone per contribuire all'efficacia dell'ISMS

Il Gruppo Applied ha identificato il **modello organizzativo relativo alla gestione della sicurezza delle informazioni** riportato di seguito:



8.1 Comitato Direttivo

Ruolo primario in Applied e tra le attività dirette di propria competenza, indirizza strategicamente le attività di approvazione del budget necessario a garantire il giusto livello di risorse per l'implementazione, manutenzione e continuo miglioramento dell'ISMS.

8.2 Head of P & S Committee

All'interno della propria responsabilità sull'area, indirizza le linee guide e le policy in ambito Information Security, in accordo con il Cyber Security & Compliance Manager affinché siano chiari gli obiettivi. Partecipa attivamente alle attività di risk assessment ed è il responsabile diretto del Cyber Security & Compliance Manager e primo approvatore della documentazione dell'Information Security Management System.

8.3 Head of Staff

All'interno della propria responsabilità sull'area, indirizza le linee guide e le policy in ambito Information Security attraverso:

- Indirizzo strategico delle attività, in accordo con il Cyber Security Manager, per stabilire i criteri di sicurezza in relazione agli ambiti legati ai Servizi Generali e People;

- Assicura, attraverso il continuo monitoraggio, che tutte le attività indirizzate all'interno della sua area di responsabilità siano conformi ai requisiti dettate dalle politiche e dalle procedure operative e per quanto riguarda l'attuazione e la gestione delle contromisure volte alla protezione.

8.4 Cyber Security & Compliance Manager

- Identifica e definisce le politiche di sicurezza e le procedure operative, in collaborazione con i Responsabili delle Applicazioni e dell'Infrastruttura;
- Sottopone a regolare revisione ed aggiornamento la documentazione dell'ISMS;
- Diffonde la cultura di Privacy & Security, mediante l'emissione di policy e procedure all'interno della società e preservare il corretto utilizzo delle norme di sicurezza da tutti gli utenti
- Assicura che l'infrastruttura ICT dell'azienda sia adeguata al raggiungimento degli obiettivi dell'ISMS e della sicurezza delle informazioni;
- Gestisce le attività legate alla sfera Privacy e GDPR;
- Gestisce la progettualità in ambito Whistleblowing;
- Garantisce l'applicazione di adeguate misure di sicurezza alle soluzioni tecnologiche utilizzate e l'aggiornamento costante delle stesse;
- Garantisce l'implementazione e la manutenzione dei controlli di sicurezza definiti all'interno dell'ISMS;
- Conduce attività di Risk Management almeno annualmente o in caso di modifiche significative all'ISMS, evidenziando le anomalie e le aree di miglioramento identificate.
- Gestisce i security incident e si interfaccia con gli interessati
- Tiene informati i dipendenti delle proprie aree sulle attività in tema Cyber

8.5 ICT & Continuous Service Manager / Evolutive Service Manager

- Supportano il Cyber Security Manager nello stabilire i criteri di sicurezza e le procedure con la loro conoscenza degli aspetti tecnologici;
- Assicurano attraverso il continuo monitoraggio che tutte le attività indirizzate all'interno delle loro aree di responsabilità soddisfino prontamente i requisiti delle politiche e delle procedure sugli aspetti tecnologici per quanto riguarda l'attuazione e la gestione operativa delle contromisure di protezione.

- Si occupano principalmente di amministrare e gestire la tecnologia, le informazioni e i dati aziendali alla base di molteplici operazioni tecniche (riguardanti hardware, software e reti in ambienti fisici o virtuali)
- Si occupano dell'aggiornamento delle applicazioni;
- Gestiscono il ciclo di vita delle risorse tecnologiche;
- Gestiscono le operazioni di rete wireless e cablata;
- Gestiscono la sicurezza nei confronti di eventuali data breach (mediante firewall, antivirus e antispam, per esempio);
- Gestiscono la connettività mobile;
- Gestiscono la manutenzione degli elementi che costituiscono l'Infrastruttura IT;
- Effettuano il monitoraggio e pianificazione della capacità dei differenti device.