Date	Rev.	Verified	Approved
01.10.2021	**01**	✓	✓
		Dott. Paolo Franco DPO	Direzione Aziendale
	IPHNET	CF. 91365840379	
ISO 27001	ISO 27701		

Modello di organizzazione e di gestione ex Decreto Legislativo 8 giugno 2001 n. 231

Versione 2021

Art. 24-*bis* d.lgs. 231/2001 - Delitti informatici e trattamento illecito di dati		
REATI-PRESUPPOSTO	**SANZIONI PECUNIARIE**	**SANZIONI INTERDITTIVE**
Accesso abusivo ad un sistema informatico o telematico **(art. 615-*ter* c.p.)** Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche **(art. 617-*quater* c.p.)** Installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche **(art. 617-*quinquies* c.p.)** Danneggiamento di informazioni, dati e programmi informatici **(art. 635-*bis* c.p.)** Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità **(art. 635-*ter* c.p.)** Danneggiamento di sistemi informatici o telematici **(art. 635-*quater* c.p.[1])** Danneggiamento di sistemi informatici o telematici di pubblica utilità **(art. 635-*quinquies*, co. 3, c.p.[2])**	Da cento a cinquecento quote	- interdizione dall'esercizio dell'attività - sospensione o revoca delle licenze, autorizzazioni, o concessioni funzionali alla commissione dell'illecito - divieto di pubblicizzare beni e servizi

1. [1] Reato modificato dall'art. 2 comma 1 lett. o) D.Lgs. n. 7/2016

2. [2] Reato modificato dall'art. 2 comma 1 lett. p) D.Lgs. n. 7/2016

Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici **(art. 615-*quater* c.p.)** Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico **(art. 615-*quinquies* c.p.)**	Fino a trecento quote	- sospensione o revoca delle licenze, autorizzazioni o concessioni funzionali alla commissione dell'illecito - divieto di pubblicizzare beni e servizi
Falsità nei documenti informatici **(art. 491-*bis* c.p.[3])** Frode informatica del soggetto che presta servizi di certificazione di firma elettronica **(art. 640-*quinquies* c.p.)**	Fino a quattrocento quote	- divieto di contrattare con la P.A. - esclusione da agevolazioni e revoca di quelle eventualmente già concesse - divieto di pubblicizzare beni e servizi

Modello di Governance per la Privacy e la Cybersecurity

IPHNET

Sommario

1 Introduzione

1.1 Quadro normativo europeo

Il Parlamento Europeo ha approvato definitivamente, dopo un iter legislativo durato oltre quattro anni, il c.d. “pacchetto protezione dati”, che si compone di due diversi strumenti:

- Un nuovo Regolamento (“Nuovo Regolamento”) concernente la “tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati”, volto a disciplinare i trattamenti di dati personali, sia nel settore privato, sia nel settore pubblico, e destinato ad abrogare la Direttiva 95/46/CE2 (“Direttiva 95/46”) che ha portato in Italia, all’adozione del vigente D.lgs. 30 giugno 2003 n. 196 (“Codice Privacy”);
- Una nuova Direttiva (“Nuova Direttiva”) indirizzata alla “regolamentazione dei settori di prevenzione, contrasto e repressione dei crimini, nonché all’esecuzione delle sanzioni penali”, che sostituirà (e integrerà) la decisione quadro 977/2008/CE sulla protezione dei dati personali scambiati dalle autorità di polizia e giustizia (che l’Italia, peraltro, non ha ancora attuato).

La pubblicazione del Nuovo Regolamento sulla Gazzetta UE è avvenuta in data 4 maggio 2016; a partire dal ventesimo giorno dalla pubblicazione (24 maggio 2016), gli Stati membri avranno due anni di tempo per allineare la normativa nazionale alle nuove prescrizioni introdotte dal Nuovo Regolamento, che diventerà definitivamente applicabile in tutto il territorio UE a partire dal 25 maggio 2018.

Per quel che concerne la Nuova Direttiva, gli Stati membri avranno due anni per recepire con apposite norme le sue disposizioni all’interno dell’ordinamento nazionale.

Il nuovo “pacchetto protezione dati” mira ad adeguare la data protection rispetto all’evoluzione tecnologica che ha determinato un aumento dei flussi transfrontalieri e, quindi, dei dati scambiati tra attori pubblici e privati, rendendo così necessari: da un lato, una più libera circolazione di dati all’interno dell’UE ma, dall’altro, un più elevato livello di protezione. Merita altresì porre in rilievo la forte volontà del Legislatore europeo di eliminare la frammentazione applicativa della normativa in materia di protezione dei dati personali nel territorio dell’UE, dovuta alle diverse leggi di recepimento della Direttiva 95/46.

1.2 Sicurezza delle informazioni

La sicurezza delle informazioni aziendali rappresenta un ambito che è diventato fonte di preoccupazione crescente per tutte le aziende.

Diventa quindi imprescindibile per IPHNET proteggere i dati strategici, ossia l’insieme di file, informazioni e documenti che costituiscono un patrimonio da tutelare in tutti i suoi aspetti.

L’uso (e l’abuso) di nuove tecnologie di IPHNET ai dati strategici aziendali rischia di introdurre nuove

minacce e nuove vulnerabilità. L'impatto derivante dal verificarsi di una delle tante minacce o vulnerabilità rischia di avere conseguenze importanti sul business dell'azienda o sulla sua credibilità nel mercato di riferimento.

2 Principali cambiamenti

Il Regolamento Europeo per la Protezione dei Dati introduce nuove tutele a favore degli interessati, e inevitabilmente nuovi obblighi a carico di Titolari e Responsabili del trattamento di dati personali. Si segnala l'introduzione del diritto dell'interessato alla "portabilità del dato" (ad. es. nel caso in cui si intendesse trasferire i propri dati da un social network ad un altro) e del diritto all'oblio per cui ogni individuo potrà richiedere la cancellazione dei propri dati in possesso di terzi (per motivazioni legittime). Questo potrà accadere ad esempio in ambito web quando un utente richiederà l'eliminazione dei propri dati in possesso di altro servizio web.

Per Titolari e Responsabili del trattamento le novità saranno molte, ad esempio:

- Il principio della accountability comporterà l'onere di dimostrare l'adozione, senza convenzionalismi, di tutte le misure privacy adottate nel rispetto del Regolamento Europeo.
- bisognerà redigere e conservare opportune documentazioni quali i Registri delle attività di trattamento (art. 30) in cui vengano riportate tutte le attività di trattamento dati svolte sotto la responsabilità del titolare al trattamento o del responsabile.
- viene richiesto di cooperare con l'autorità di controllo notificando qualsiasi violazione dei dati personali alla stessa e al diretto interessato (artt. 32-34).
- saranno necessarie valutazioni d'impatto sulla protezione dei dati, o Privacy Impact Assessment (art. 35) in caso di trattamenti rischiosi, e verifiche preliminari per diverse circostanze da parte del Garante.
- Adozione di metodologie di privacy by design e by default che possano assicurare che i controlli, le procedure e le tematiche di tutela dei dati personali facciano parte della vita quotidiana dell'azienda sia per i dati di cui è direttamente responsabile che per quelli sui quali svolge il ruolo di responsabile esterno.
- Definire un responsabile per il trattamento dei dati che possa aiutare l'azienda ad individuare le politiche più adatte e fornire le metodologie più sicure per la tutela dei dati

3 Obiettivi

Comer riconosce che il contesto normativo europeo è notevolmente cambiato ponendo l'accento alla tutela dei propri dati personali e strategici.

In questo nuovo contesto IPHNET vuole fornire una risposta adeguata ai cambiamenti normativi e vuole, allo stesso tempo, dare forza alle azioni di tutela dei dati personali integrando gli sforzi da compiere nell'ambito dei sistemi di gestione di cui si è dotata.

In questo contesto IPHNET stabilisce che il modo più opportuno per:

[1] essere conforme al nuovo contesto normativo

[2] garantire la tutela dei dati personali dei dipendenti e
[3] integrare le misure intraprese sull'Information Security è

di adottare un **Modello di Governance per la Privacy e la Cybersecurity.**

4 Modello di Governance

Il Modello di Governance è l'insieme delle politiche, delle metodologie e dei processi atti a tutelare i dati personali e strategici nell'ambito di tutte le funzioni operanti nei processi di IPHNET.

Il modello di governance si basa sui seguenti capitoli:

1. Organizzazione
2. Policy
3. Registro dei trattamenti
4. Diritti dell'interessato
5. Gestione del rischio
6. Misure di sicurezza
7. Continuità operativa
8. Gestione delle terze parti
9. Gestione degli incidenti
10. Conformità e miglioramenti

Ogni capitolo è studiato per rispondere a determinati articoli presenti in:

- Regolamento UE 2016/679, di seguito anche GDPR, per la privacy dei dati personali
- ISO 27001/2017 per la protezione dei dati strategici (ad es. brevetti, proprietà intellettuale, progetti, piani strategici, etc.)

4.1 Organizzazione e ruoli

Il Team creato da IPHNET in questo modello di governance è chiamato Privacy e Cybersecurity Team. Questo è costituito da un livello accountable, dove risiedono i responsabili per i dati personali e strategici, ed uno responsible, dove risiedono le figure che operativamente implementano controllano e mantengono il modello.

L'organizzazione di IPHNET a tutela dei dati personali e strategici si basa sull'organigramma descritto di seguito:

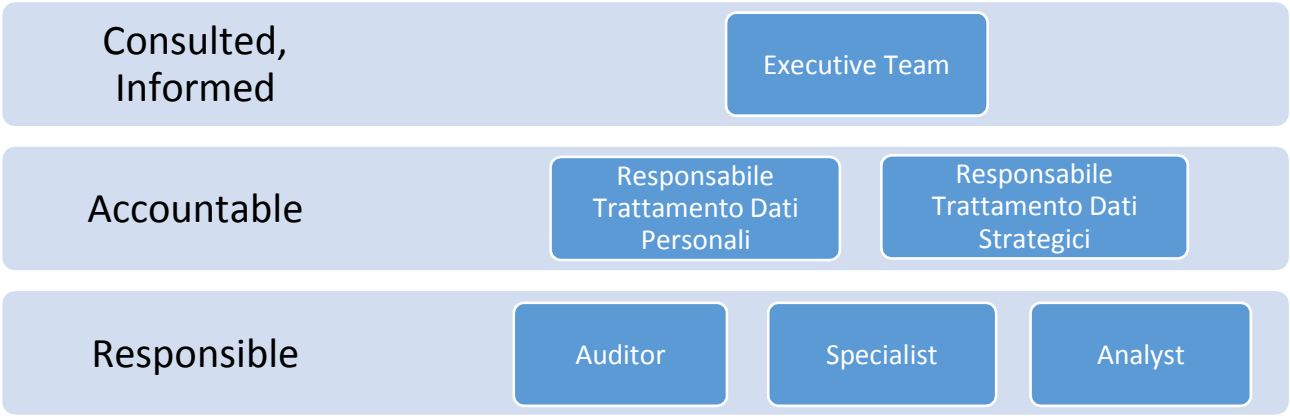

Figura 1: organizzazione di privacy e cybersecurity

L'organizzazione logica descritta in precedenza ha una corrispondenza con personale interno di IPHNET già appartenente a gruppi di lavoro esistenti.

I ruoli sono distribuiti nel modo seguente:

- Executive Team: costituito dai primi riporti dell'AD di IPHNET che viene consultato e/o informato su tutte le tematiche relative alla privacy e cybersecurity. Il Team si occupa anche di approvare le politiche e sponsorizzare le attività necessarie;
- Responsabile trattamento dei dati personali: è il responsabile IPHNET per il trattamento dei dati personali;
- Responsabile trattamento dati strategici: è il responsabile IPHNET per il trattamento e misure di sicurezza tecnologiche da adottare per proteggere i dati strategici aziendali;
- Auditor: è la figura che operativamente si occupa di effettuare l'audit sulla protezione dei dati personali e dei dati strategici. Non è detto che i due audit vengano effettuati dalla stessa persona;
- Specialist: è la figura con profilo adeguato per gestire la sicurezza tecnologica dei dati IPHNET (sia personali che strategici) e la loro applicazione a progetti, applicazioni e ambiti di lavoro;
- Analyst: è la figura che è in grado di collaborare e cooperare con tutte le funzioni di IPHNET per risolvere tematiche di gestione e protezione dei dati

4.1.1 TITOLARE DEL TRATTAMENTO

Il Titolare del Trattamento è la persona fisica, la persona giuridica, la Pubblica Amministrazione e qualsiasi altro ente, associazione o organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.

Il Titolare del Trattamento dei dati personali contenuti nelle banche dati è individuato nella Associazione iphnet con sede legale ed amministrativa Via Lorenzo il Magnifico 42 00162 Roma. Il Titolare del trattamento affida ai singoli Responsabili del Trattamento dei dati il compito di porre in essere ogni

misura tesa a ridurre al minimo il rischio di distruzione dei dati, l'accesso non autorizzato o il trattamento non consentito, previe idonee istruzioni fornite con ogni mezzo ritenuto più idoneo.

Il Titolare del Trattamento affida ai singoli Responsabili del Trattamento dei dati il compito di individuare, nominare e indicare per iscritto uno o più incaricati del trattamento.

4.1.2 RESPONSABILE DEL TRATTAMENTO

Il Responsabile del trattamento è nominato dal Titolare, sulla base di precise istruzioni scritte, e ha espressamente accettato la designazione.

Il Responsabile del trattamento è informato dell'obbligo di conformarsi in ogni caso, per quanto di propria competenza, a tutte le istruzioni relative al trattamento dei dati personali contenute nei vari documenti aziendali, ancorché ulteriori rispetto alle istruzioni impartite nelle rispettive lettere di designazione.

Nel caso di cambiamenti della organizzazione aziendale è senza indugio verificata l'opportunità di procedere all'aggiornamento delle designazioni per adeguarle eventualmente alle nuove esigenze organizzative.

4.1.3 INCARICATI DEL TRATTAMENTO

Il personale che esegue operazioni di trattamento di dati personali è designato Incaricato del trattamento.

La designazione degli Incaricati del trattamento è eseguita da parte del Titolare ovvero dal Responsabile del trattamento, per quanto di propria competenza, attraverso lettere di conferimento di incarico.

La designazione degli Incaricati rinvia, per quanto riguarda l'ambito del trattamento consentito, alle categorie di dati personali e alle operazioni consentite nella funzione aziendale nella quale opera l'Incaricato.

L'individuazione dell'ambito del trattamento consentito ai singoli Incaricati è aggiornato annualmente.

Le lettere sono restituite dagli incaricati, sottoscritte per presa visione, alla Direzione del personale, che ne cura la conservazione.

In caso di trasferimento ad altra funzione aziendale dell'Incaricato del trattamento, esso è immediatamente informato dell'ambito del trattamento consentito nella nuova funzione aziendale ed è modificato il sistema di autorizzazione per l'accesso ai dati personali che lo riguarda.

4.1.4 AMMINISTRATORI DEL SISTEMA

L'amministratore del Sistema è il soggetto cui è conferito il compito di sovrintendere alle risorse del sistema operativo degli elaboratori della rete e di consentirne l'utilizzazione. È compito dell'amministratore del sistema:

- predisporre ogni provvedimento necessario ad evitare la perdita o la distruzione dei dati e provvedere al ricovero periodico degli stessi con copie di back-up;
- assicurarsi della qualità delle copie di back-up dei dati e della loro conservazione in luogo adatto e sicuro;

- Fare in modo che sia prevista la disattivazione delle credenziali di autenticazione (abbinamento user-id e password) in caso di perdita della qualità che consentiva all'utente/incaricato l'accesso al sistema di elaboratori, oppure nel caso di mancato utilizzo delle credenziali per oltre 6 mesi;
- Proteggere gli elaboratori dal rischio di intrusione (violazione del sistema da parte di "Hacker") e dal rischio di virus mediante idonei programmi.

Gli Amministratori del Sistema sono identificati nei responsabili di settore dell'area Sistemi Informativi e dei fornitori di servizio preposti. La nomina di Amministratore del Sistema può essere revocata in qualsiasi momento dal Responsabile del Trattamento anche senza preavviso.

Gli accessi degli amministratori di rete ai server contenenti dati personali sono loggati su un server centralizzato.

Per i sistemi in outsourcing la gestione degli accessi degli amministratori è dettagliata nel "Manuale delle Operazioni" che regolamenta il suddetto servizio.

Per maggiori informazioni sull'organigramma, ruoli e responsabilità del team di Privacy e Cybersecurity fare riferimento alla sezione apposita creata nel SITO WEB

Gli articoli del GDPR coperti da questo ambito sono:

Tematica	**Articolo**
Titolare del trattamento	24
Contitolari del trattamento	26
Responsabile del trattamento	28
Codice di condotta o certificazioni	40, 42
Rappresentanti di Titolari o Responsabili del trattamento non stabiliti nell'Unione	27

Tabella 1 Riferimenti articoli GDPR – Organizzazione

Le clausole della ISO 27001 coperti da questo ambito sono:

Tematica	**Clausola**
Organisation of information security	6

Tabella 2 Riferimenti clausole ISO27001 – Organizzazione

4.2 Policy per la privacy e cybersecurity

Le politiche di sicurezza dei dati (sia personali che strategici) hanno lo scopo di definire le linee guida per garantire l'integrità, disponibilità e riservatezza dei dati aziendali da minacce e vulnerabilità.

Le linee guida principali nella definizione e applicazione delle Politiche di Sicurezza sono:

- Standardizzazione: Una protezione globale è possibile solo se tutti i componenti della catena si caratterizzano per lo stesso livello di sicurezza. È quindi necessario definire e implementare un livello standard di sicurezza per workstation, server, sistemi,

servizi, processi, risorse, reti e applicazioni.
- Integrazione: Ogni progetto che coinvolge IPHNET deve rispettare i requisiti di sicurezza.

- Applicabilità: Ogni dispositivo di sicurezza da implementare deve caratterizzarsi per una procedura semplice e una struttura compatibile con l'organizzazione dell'azienda o delle consociate.
- Idoneità: Ogni dispositivo di sicurezza utilizzato deve essere proporzionato ai rischi identificati e all'ambiente applicativo.
- Durevolezza: Le misure di sicurezza prescelte devono basarsi su tecnologie consolidate, innovative e semplici da mantenere.
- Monitoraggio: I dispositivi di sicurezza prescelti devono essere in grado di registrare un qualunque evento che possa incidere sulla protezione o sul corretto funzionamento dei sistemi in questione.

Gli articoli del GDPR coperti da questo ambito sono:

Tematica	**Articolo**
Policy in materia di protezione dei dati personali	5, 24, 91
Policy sul trattamento di dati sensibili e giudiziari	6, 9, 10
Identificazione dei requisiti di compliance	39
Policy e procedure di pseudonimizzazione dei dati	89
Policy e procedure sulla conservazione dei dati	5
Policy e procedure sull'utilizzo sicuro delle risorse informatiche	32
Training su tematiche privacy	39

Tabella 3 Riferimenti articoli GDPR – policy per privacy

Le clausole della ISO 27001 coperti da questo ambito sono:

Tematica	**Clausola**
Security Policy	5

Tabella 4 Riferimenti clausole ISO27001 – policy cybersecurity

4.3 Registro dei trattamenti

Il registro delle attività di trattamento dei dati personali è un punto cardine per IPHNET.

La soluzione più adeguata individuata al supporto del registro consiste in un database in cui

sono mantenute e aggiornate le seguenti informazioni:

- Nome del trattamento
- Descrizione del trattamento
- Responsabile del Trattamento
- Finalità del trattamento

- Descrizione delle categorie di Interessati
- Categorie di dati personali
- Descrizione dei dati personali trattati
- Personale autorizzato ad accedere ai dati
- Categorie di destinatari
- Modalità di trattamento
- Gestione informativa
- Raccolta consenso
- (Opzionale) Responsabile del Trattamento Esterno
- (Opzionale) Elenco Fornitori e sub-fornitori
- (Opzionale) Trasferimenti verso paesi terzi o organizzazioni internazionali
- Termini ultimi previsti di cancellazione
- Sistema IT che gestisce i dati
- Descrizione generale delle misure di sicurezza adottate
- Locazione fisica del sistema/applicazione

Il registro dei trattamenti è gestito dal DPO di Privacy e Cybersecurity e viene revisionato annualmente e aggiornato in caso di cambiamenti in una delle categorie elencate in precedenza.

4.3.1 Classificazione dei dati

Alla base della gestione dei dati (o più in generale degli asset) c'è la loro classificazione. Comer descrive in una policy quali sono i livelli di classificazione delle informazioni.

Principalmente si suddividono due categorie di dati:

[1] Personali: qualsiasi informazione (nome, codice fiscale, immagine, voce, impronta digitale, traffico telefonico) concernente una persona fisica identificata o identificabile, anche indirettamente, oppure informazioni riguardanti una persona la cui identità è nota o può comunque essere accertata mediante informazioni suplementari

[2] Strategici: qualsiasi informazione che non ricade nella categoria precedente e riguarda le attività di amministrazione, sviluppo, ricerca, vendita, supporto, comunicazione, marketing, finanza, gestione, controllo e tutte le altre funzioni che Comer svolte quotidianamente per propria mission aziendale;

Comer ha identificato le seguenti categorie di dati personali ai quali applicare le regole di protezione disposte dal GDPR:

- Fornitori;
- Clienti;
- Consulenti/collaboratori;
- Soci, Amministratore Unico;
- Visitatori/ospiti/altri;

Gli articoli del GDPR coperti da questo ambito sono:

Tematica	Articolo
Registro delle attività di trattamento	30
Aggiornamento del registro	30
Trasferimenti dei dati verso paese terzo	45, 46, 49

Tabella 5 Riferimenti articoli GDPR – registro attività

Le clausole della ISO 27001 coperti da questo ambito sono:

Tematica	Clausola
Asset management	5

Tabella 6 Riferimenti clausole ISO27001 – registro attività

4.4 Diritti dell'interessato

Il GDPR ha reso la trasparenza uno degli aspetti più importanti da garantire agli interessati dei quali si trattano i dati personali.

Comer segue le indicazioni fornite dal Garante per la Privacy e riprese dal GDPR che individuano nell'informativa per la Privacy il primo passo per legittimare trattamenti e garantire l'esercizio dei diritti dell'interessato.

L'informativa, preferibilmente scritta e firmata dagli interessati, include queste informazioni:

- le finalità del trattamento;
- le categorie di dati personali in questione;
- i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;
- quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare questo periodo;
- l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento;
- il diritto di proporre reclamo ad un'autorità di controllo;
- qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;
- l'esistenza di un processo decisionale automatizzato, compresa la profilazione e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

Gli articoli del GDPR coperti da questo ambito sono:

Tematica	Articolo
Template e linee guida sull'informativa sulla privacy	8, 13, 14
Revisione template su informativa	13, 14
Comunicazione dell'informativa sulla privacy	13, 14, 21
Procedure per la raccolta del consenso	6, 7, 8
Trattamenti per finalità diverse da quelle originarie	6, 13, 14
Trattamento dei dati sui minori	8, 12
Trattamento per finalità di marketing diretto	21
Procedure di verifica dell'identità dell'interessato	15, 16, 17, 18, 20, 21, 22
Procedure per richiesta di revoca al trattamento	7 (3)
Procedure per richiesta di conferma sull'utilizzo e accesso ai dati personali	15
Procedure per richiesta di rettifica dei dati personali	16
Procedure per richiesta di limitazione al trattamento	18
Procedure per richiesta di portabilità dei propri dati	20
Procedure per revisione dei processi decisionali automatizzati	22
Procedure per richiesta cancellazione (diritto all'oblio)	17
Procedura di cancellazione del dato	17, 20, 21
Procedure di rettifica o cancellazione dei dati personali o limitazione del trattamento	19

Tabella 7 Riferimenti articoli GDPR – diritti dell’interessato

Le clausole della ISO 27001 coperti da questo ambito sono:

Tematica	Clausola
N/A	N/A

Tabella 8 Riferimenti clausole ISO27001 – diritti interessato

4.5 Gestione del rischio

La gestione degli impatti sulla privacy e dei rischi sui dati personali segue le tematiche della metodologia di Information Security (ISO 27001), come riportato di seguito:

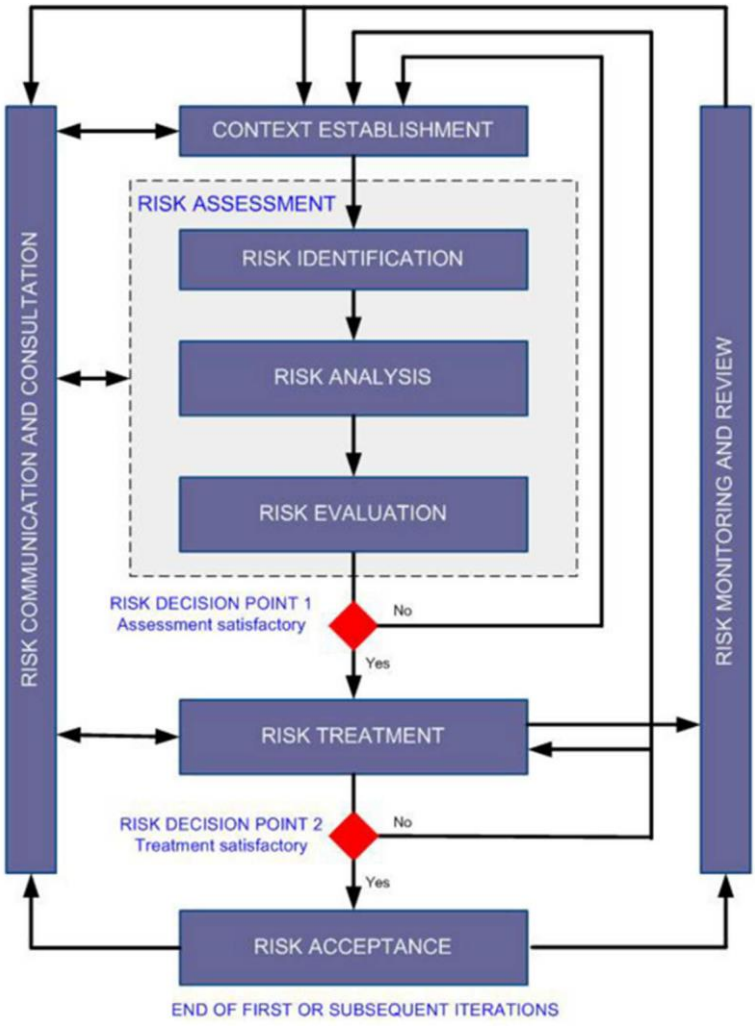

Figura 2 – processo di risk management

Questo processo è stato adattato al caso della valutazione di impatti e rischi legati ai trattamenti dei dati personali (sia interni che esterni).

Per una descrizione del processo fare riferimento ai documenti di politica e processo di risk management nell'apposito sito Intranet di IPHNET

L'analisi dei rischi è stata condotta in modo ampio ed esaustivo analizzando anche eventi tecnici ed organizzativi più ampi rispetto alle prescrizioni legislative; e ciò anche in considerazione delle previsioni dell'art.31 del Testo Unico e del richiamato art.2050 del c.c.

L’analisi, naturalmente, è stata principalmente focalizzata sulle circostanze possibili o probabili che possano costituire il verificarsi di rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

L'esame dei rischi è stato fatto anche in relazione alla natura dei dati, distinguendo tra i dati personali ordinari e quelli particolari, nonché delle caratteristiche del trattamento.

Tutti i rischi esaminati sono stati individuati, classificati e descritti, nei seguenti principali raggruppamenti:

- rischi specifici,
- rischi sull’integrità dei dati,
- rischi sulla riservatezza dei dati, di trattamenti non consentiti o non conformi alle finalità della raccolta,
- rischi sulla disponibilità dei dati.

L’analisi dei rischi descrive gli eventi potenzialmente dannosi per la sicurezza dei dati e ne valuta le possibili conseguenze e gravità in relazione al contesto fisico-ambientale di riferimento e agli strumenti utilizzati. Si propone di individuare un insieme di misure di protezione, commisurate alle reali necessità di sicurezza, da adottare nell’ambito del perimetro d’intervento ovvero dell’area di analisi.

Per una valutazione dei rischi, eseguito sui processi di Comer, si rimanda all’assessment di IPHNET

Gli articoli del GDPR coperti da questo ambito sono:

Tematica	**Articolo**
Assessments privacy	24, 39
Data protection by design and by default	25
Integrazione della data privacy nelle attività di risk assessment	32
Esecuzione di DPIA per nuove applicazioni/sistemi/processi	5, 6, 25, 35
Linee guida e template su analisi del rischio sulla protezione dei dati (DPIA)	35
Esecuzione di DPIA su change ad applicazioni/sistemi/processi esistenti	5, 6, 25, 35(11)
Ingaggio di personale esterno su DPIA	35
Tracciamento delle azioni di remediation sulle criticità identificate dal DPIA	35
Consultazione preventiva	36

Tabella 9 Riferimenti articoli GDPR – gestione del rischio

Le clausole della ISO 27001 coperti da questo ambito sono:

Tematica	Clausola
Tutta ISO 27001	Tutte

Tabella 10 Riferimenti clausole ISO27001 – gestione del rischio

4.6 Misure di sicurezza

Le misure a protezione dei dati personali rappresenta l'ambito di maggior interesse per la ISO 27001. L'elenco delle misure a protezione delle informazioni (che includono i dati personali) sono riportate di seguito.

4.6.1 Aree e locali

Di seguito sono sinteticamente riportati i criteri tecnici ed organizzativi per la protezione delle aree e dei locali interessati alle misure di sicurezza nonché le procedure per controllare l'accesso delle persone autorizzate ai locali medesimi:

- Gli stabili dispongono di ingressi dotati di sorveglianza.
- Le regole di accesso sono definite mediante apposita normativa disponibile anche presso la reception.
- I dati relativi alle registrazioni sono accessibili solo ad alcuni incaricati specificatamente designati. Le registrazioni vengono di norma conservate per un periodo limitato, salvo casi di accertata anomalia. In tal caso sono riversate su un supporto rimovibile (nastro o CD) e conservate in cassaforte in previsione di un possibile utilizzo in sede giudiziale.

4.6.2 Integrità dei dati

Per garantire l'integrità dei dati, IPHNET applica al proprio modello di governance le regole seguenti:

- Tutte le procedure che vengono inserite in ambiente di produzione devono superare una fase di test in apposito ambiente come prescritto nelle normative interne. La società esterna incaricata dello sviluppo e manutenzione del software è sottoposta a continua verifica di qualità e ogni prodotto rilasciato è accompagnato dal verbale di accettazione, che comprende la descrizione di tutte le attività di test effettuate e del relativo esito.
- Tutto il personale che deve operare dispone di una documentazione adeguata ed ha seguito appositi corsi di formazione o dispone di una pluriennale esperienza.
- Per ogni informazione viene tenuta una copia di back up e sono effettuate registrazioni su sistemi differenti in modo da poter permettere la ricostruzione dei dati a fronte di cancellazioni o danneggiamenti.

- Per evitare perdite accidentali si ricorre al minimo a comandi manuali utilizzando sistemi automatici.
- Per minimizzare eventuali problemi dovuti a guasti hardware, dove possibile, si provvede ad una costante manutenzione degli apparecchi.
- Il software potenzialmente pericoloso (utility di sistema) viene controllato dal sistema automatico di protezione logica degli accessi che ne limita l'utilizzo al solo personale autorizzato.

4.6.3 Disponibilità dei dati

Comer ha identificato le seguenti misure per garantire la disponibilità dei propri dati (sia personali che strategici):

- Architettura della rete di trasmissione dei dati (ridondanze e istradamenti alternativi). Autonomia per l'alimentazione elettrica .
- Fornitura di elettricità tramite differenti cabine elettriche. Piano di continuità del servizio.
- Procedure realizzate con la caratteristica di una disponibilità 7x24.
- Si utilizzano collegamenti in fibra ottica con backup HDSL ed HDSL doppi in bilanciamento di carico.
- Le batterie di emergenza dei sistemi centrali hanno una capacità tale da consentire il funzionamento del sistema, durante i quali il generatore di emergenza si avvia ed è in grado di fornire energia al sistema di elaborazione dati.

4.6.4 Riservatezza dei dati

Di seguito vengono sintetizzati i criteri e le procedure per la sicurezza delle trasmissioni dei dati, ivi compresi quelli per le restrizioni di accesso per via telematica.

- Tutti gli strumenti dai quali si può accedere ai dati sono censiti e codificati. Le autorizzazioni non si riferiscono mai a tali strumenti bensì ai singoli operatori.
- Con opportuni strumenti di analisi è possibile risalire ai dati relativi al sistema e all'operatore o al gruppo che hanno eseguito una specifica operazione.
- I sistemi automatici che accedono ai dati (p.e. programmi di tipo batch) sono singolarmente autorizzati e si presentano con un proprio identificativo (nome del programma).
- Le autorizzazioni seguono strettamente la politica del "minimo privilegio" e sono legate al reale bisogno di accesso e trattamento dei dati.
- Tutte le autorizzazioni sono sottoposte a verifica periodica in relazione alla permanenza delle necessità di accesso.
- Le autorizzazioni vengono gestite mediante gruppi definiti in base a criteri "need to know".
- Le richieste di autorizzazione per utenti esterni possono pervenire solo da responsabili incaricati per delega.
- Le credenziali di accesso vengono richieste tramite form automatizzato ed autorizzate tramite workflow approvativo secondo la procedure di gestione utenze.

Le utenze vengono dismesse dopo ricezione della comunicazione HR. Le modifiche ai permessi di accesso vengono richieste tramite ticket ed applicate solo dopo idonea autorizzazione.

4.6.5 Sicurezza delle trasmissioni dei dati

La connessione con l'esterno avviene tramite linee differenziate .

I documenti contenenti dati personali o riservati sono in cartelle del file server. Ogni utente dispone della propria cartella, a cui può accedere solo dopo ave digitato il proprio codice identificativo e la password. Le cartelle sono personali (cioè accessibili solo all'utente) o relative all'ufficio . Per rendere la gestione delle password aderente ai requisiti imposti dal GDPR, la procedura di accesso prevede l'impiego dei servizi di autenticazione del sistema operativo del computer client per garantire l'accesso agli utenti e consentire successivamente, solo a quelli abilitati, la connessione alle risorse di rete. La sicurezza e l'aderenza ai requisiti imposti dal GDPR sulle misure adeguate è garantita dal fatto che sui Personal Computer il sistema operativo impedisce l'accesso senza aver prima superato con successo le fasi di login.

La protezione dell'integrità dei dati che viaggiano sulla rete è affidata al software di gestione dei servizi LAN. Tutte le connessioni della INTRANET con la rete INTERNET sono protette tramite apposito dispositivo (firewall) che impedisce accessi non autorizzati. Le connessioni con l'esterno sono soltanto quelle con la rete INTERNET adeguatamente protetta.

Come principio generale l'installazione di modem per comunicazione su linee commutate è proibito. E' proibito inoltre l'utilizzo dei modem presenti sui personal computer portatili con le eccezioni relative alle connessioni tramite VPN aziendali.

Singole autorizzazioni sono concesse a fronte di esigenze che non sono risolvibili con altre tipologie, quali ad esempio:

- modem o connect card che consentono l'accesso per il lavoro svolto da dipendenti autorizzati presso il loro domicilio
- modem che abilitano l'accesso da linea commutata per alcune società esterne che scaricano dati (es. banche). In questi casi l'accesso è protetto da appositi sistemi.

Gli articoli del GDPR coperti da questo ambito sono:

Tematica	**Articolo**
Misure tecniche di sicurezza (e.g. intrusion detection, firewalls, monitoring)	32
Inventario dei dati mantenuti	30, 32
Modalità di cifratura o anonimizzazione dei dati	25, 32
Procedure di back-up e ripristino dei dati	32

Procedure di controllo accesso ai dati personali	32
Esecuzione di attività di test di sicurezza	32

Tabella 11 Riferimenti articoli GDPR – misure di sicurezza

Le clausole della ISO 27001 coperti da questo ambito sono:

Tematica	**Clausola**
Access control	9
Cryptography	10
Physical and environmental security	11
Operations security	12
Communications security	13
System acquisition. development and maintenance	14

Tabella 12 Riferimenti clausole ISO27001 – misure di sicurezza

4.7 Continuità operativa

La continuità operativa è essenziale per garantire che tutte le misure attuate a protezione di dati (sia personali che strategici) siano resilienti ad incidenti che possono degradare il livello di servizio.

Comer ha affrontato la continuità operativa di infrastrutture, sistemi e applicativi operando su due livelli distinti:

- On-premise:
  - nella sede di Roma sono state implementate misure di ridondanza su tutti i sistemi adottati per garantire ai servizi ospitati di essere fault tollerant. Ad esempio:
    - i sistemi di storage prevedono tecniche di ridondanza
    - è presente un sistema di monitoraggio real-time;
    - esecuzione di backup ;
    - esiste un sistema di inventario e gestione ;
    - esiste un sistema centralizzato, basato su Windows Defender, di protezione avanzata da malware sia per server che per client con aggiornamento quotidiano delle definizioni dell'elenco di virus, trojan, zero-day attack e in generale per tutti i malware;;
    - Per gli utenti esterni alla rete è garantita una connessione protetta alla rete aziendale tramite VPN ipsec che garantisce la verifica degli

account, delle autorizzazioni e del controllo del traffico tramite cifratura SSL;

Gli articoli del GDPR coperti da questo ambito sono:

Tematica	**Articolo**
Misure tecniche di sicurezza (e.g. intrusion detection, firewalls, monitoring)	32

Tabella 13 Riferimenti articoli GDPR – misure di sicurezza

Le clausole della ISO 27001 coperti da questo ambito sono:

Tematica	**Clausola**
Business continuity of information security	16

Tabella 14 Riferimenti clausole ISO27001 – misure di sicurezza

4.8 Gestione dei fornitori

La gestione dei fornitori, prevista nel modello per la privacy e cybersecurity, si basa sulla compilazione di checklist studiate per valutare il grado di compliance rispetto alla protezione dei dati.

Le checklist create consentono di valutare:

[1] l'adeguatezza dei contratti siglati con le terze parti;
[2] il livello di cybersecurity (rispetto alle clausole della ISO27001) e,
[3] il livello di adozione del GDPR.

Per maggiori informazioni sui template degli assessment o i risultati degli stessi si rimanda all'apposita sezione presente sul sito Intranet di IPHNET

Gli articoli del GDPR coperti da questo ambito sono:

Tematica	**Articolo**
Definizione requisiti Privacy con le terze parti	28(3), 32
Revisioni contratti o stipula di nuovi contratti con terze parti	28
Contratti con sub-fornitori	28(4)
Verifica delle referenze e garanzie nella scelta di fornitori e responsabili del trattamento	28(1)
Autorizzazioni per ricorso ad ulteriori Responsabili del trattamento	28(2)
Termine del contratto	28(3)(g)

Tabella 15 Riferimenti articoli GDPR – gestione terze parti

Le clausole della ISO 27001 coperti da questo ambito sono:

Tematica	**Clausola**
Supplier relationship	15

Tabella 16 Riferimenti clausole ISO27001 – gestione terze parti

4.9 Gestione degli incidenti

Di seguito viene riportato il flusso di processo di gestione degli incidenti applicati sia alla sicurezza delle informazioni che tutela dei dati personali:

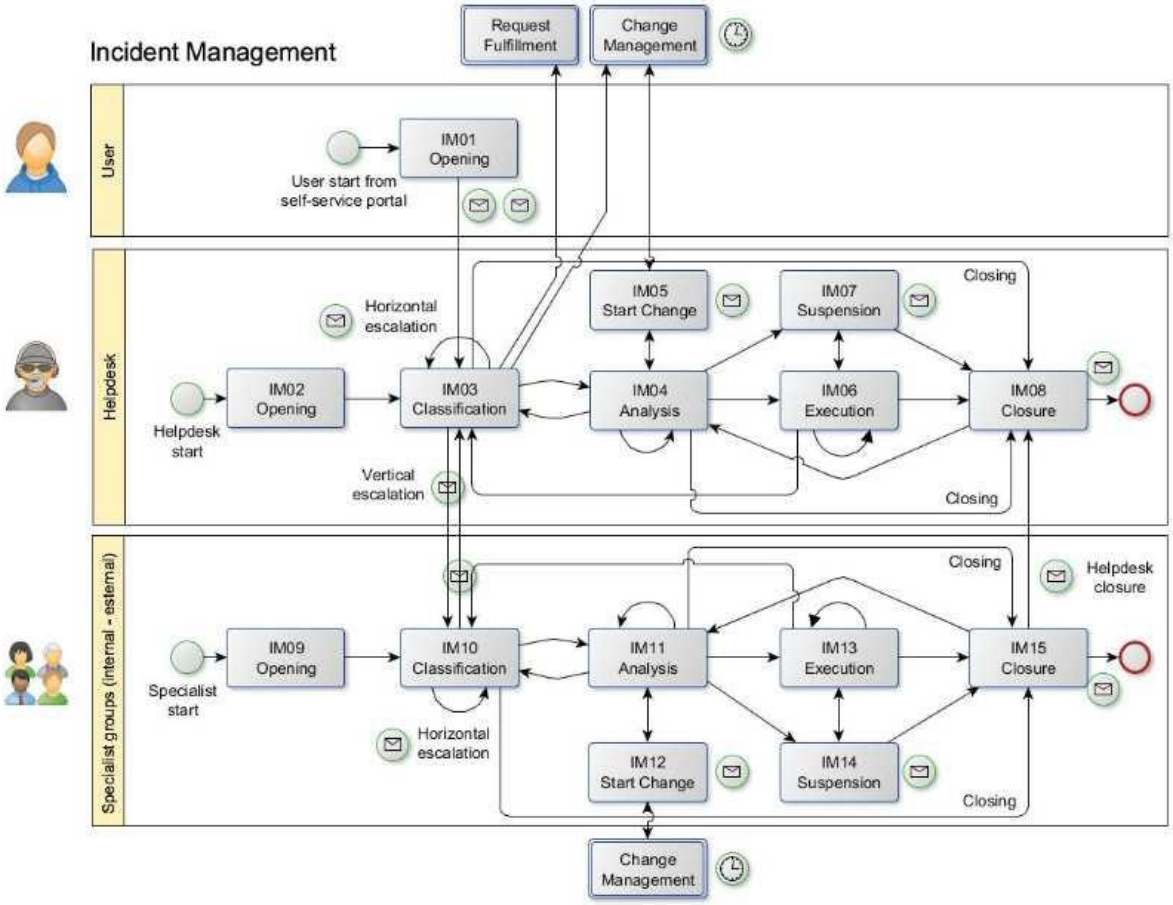

Figura 3 – processo di gestione degli incidenti

Le fasi mostrate nella figura sono descritte di seguito:

- IM01: l'utente apre un incident
- IM02: l'help desk apre un incident
- IM03: l'help desk classifica l'incidente
- IM04: l'help desk effettua una prima classificazione dell'incidente
- IM05: l'help desk apre un change se l'analisi lo richiede
- IM06: (se possibile) l'help desk esegue una procedura per la risoluzione dell'incidente
- IM07: l'help desk sospende la risoluzione dell'incident se richiesto
- IM08: l'help desk chiude l'incident se considerato risolto
- IM09: il gruppo specialistico apre un ticket per un incident
- IM10: il gruppo specialistico classifica l'incident
- IM11: il gruppo specialistico analizza l'incident
- IM12: Il gruppo specialistico richiede un change per la risoluzione dell'incident

- IM13: il gruppo specialistico esegue una procedura per la risoluzione dell'incident
- IM14: IL gruppo specialistico sospende la risoluzione dell'incident
- IM15: il gruppo specialistico chiude l'incident

Si rimanda ai documenti relativi alla politica per la gestione degli incidenti e alla descrizione del processo di incident management per maggiori informazioni

Gli articoli del GDPR coperti da questo ambito sono:

Tematica	**Articolo**
Template per notifica di data breach	33(3)
Training su procedure di escalation	33
Policy di gestione degli incident	33, 34
Notifica violazione dei dati personali alle autorità di controllo	33, 34
Comunicazione di violazione dei dati personali agli interessati	12, 33, 34
Contratti con le terze parti	33(2)
Documentazione delle violazioni dei dati personali	33(5)

Tabella 17 Riferimenti articoli GDPR – data breach

Le clausole della ISO 27001 coperti da questo ambito sono:

Tematica	**Clausola**
Information security incident	16

Tabella 18 Riferimenti clausole ISO27001 – incidenti

4.10 Conformità e miglioramenti

Il modello di governance prevede al suo interno sia (i) metodi per verificare la conformità di processi, sistemi o applicazioni agli standard di Privacy e Cybersecurity, che (ii) metodi che prevedono il miglioramento continuo di tutte le sue parti (ad es. adeguamento per cambi organizzativi, allineamento alle strategie di business, adeguamento delle politiche di privacy a nuovi regolamenti, etc.).

Il modello di governance per la privacy e la cybersecurity ha due strumenti fondamentali per garantire la conformità e il miglioramento continuo:

1. Assessment tramite audit e checklist
2. Valutazione di indicatori chiave

Il primo punto è garantito da audit sia lato privacy (punti specifici del GDPR) sia lato cybersecurity (punti specifici ISO 27001). Gli audit possono essere condotti ad un livello generale che racchiude tutti i punti previsti dallo standard (in questo caso si parla di audit di

I livello), o a livello di processo (in questo caso si parla di audit di II livello) oppure su un livello di dettaglio specifico (come ad esempio un'applicazione, un sistema informativo ed in questo caso si parla di audit di III livello).

Il secondo punto è soddisfatto dalla definizione di indicatori chiave sia per la privacy che per la cybersecurity che sono valutati con cadenza semestrale o annuale (ad ogni modo a discrezione del team di Privacy e cybersecurity in accordo con l'Executive Team).

Gli indicatori includono:

- Privacy:
  - Numero di incidenti di privacy annuali: l'obiettivo è quello di ridurlo al minimo;
  - Numero di richieste degli interessati gestite entro i tempi previsti dal GDPR;: l'obiettivo è il 100%;
  - Numero di dipendenti (a tempo indeterminato o determinato) a cui viene consegnato il welcome pack: l'obiettivo è il 100%;
- Cybersecurity:
  - Numero di incidenti di security annuali: l'obiettivo di questo indicatore è quello di ridurlo al minimo;
  - Numero di sistemi/applicazioni/infrastrutture con un livello di conformità adeguato: l'obiettivo di questo indicatore è quello di raggiungere una soglia minima del 75%, il valore ideale è ovviamente il 100%;

Comer si riserva di modificare il numero e/o tipologia di indicatori chiave adeguandolo alle strategie aziendali durante la revisione annuale dei sistemi di gestione o a seguito di un incidente grave.

Le clausole della ISO 27001 coperti da questo ambito sono:

Tematica	**Clausola**
Continual Improvement	18

Tabella 19 Riferimenti clausole ISO27001 – miglioramento continuo

5 Implementazione del modello

Il modello di governance per la privacy e cybersecurity ha un'organizzazione documentale ben precisa che si rifà alle metodologie standard introdotte dalla ISO 27001 adottate dal ELCO.

La figura che segue mostra la relazione che esiste tra le tipologie di documenti e la loro funzione nell'implementazione del modello.

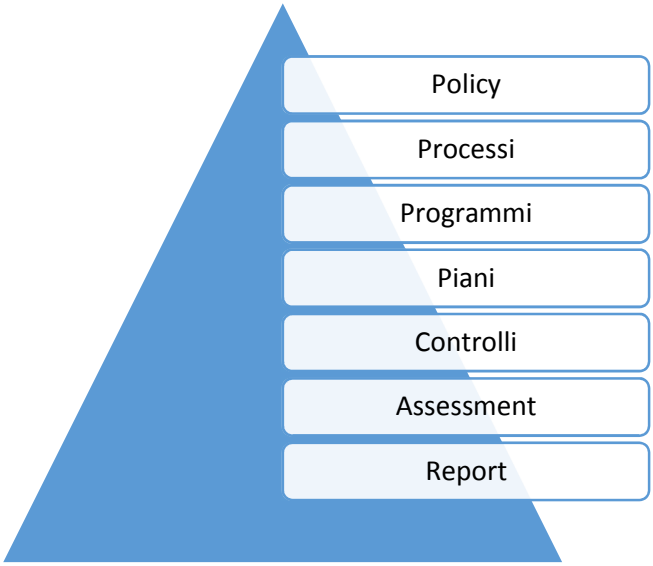

Figura 4 – implementazione del modello

Ogni elemento della piramide ha una caratteristica ben precisa:

- **Policy**: Ogni politica ha un proprietario che ha approvato la responsabilità per lo sviluppo, revisione e valutazione delle politiche. La revisione include la valutazione delle opportunità di miglioramento delle politiche dell'organizzazione e l'approccio alla gestione della sicurezza delle informazioni in risposta alle modifiche l'ambiente organizzativo, le circostanze di lavoro, le condizioni legali o ambiente tecnico.

- **Processi**: Ogni processo ha un proprietario che ha la responsabilità per lo sviluppo, revisione e valutazione dei processi. Ogni processo deve chiaramente definire l'input e output, e una serie di attività assegnate ai diversi attori coinvolti. La metrica di un processo deve garantire la valutazione dell'operato e suggerire miglioramenti al processo

- **Programmi:** Ogni programma esprime la volontà dell'azienda di schedulare a priori le attività di verifica e controllo sul sistema di gestione per la sicurezza. Il programma ha sempre un proprietario che è responsabile, in pieno accordo con le parti interessate, delle date o periodi in cui vengono effettuate le attività in oggetto.

- **Piani**: Ogni piano ha un proprietario che ha la responsabilità per lo sviluppo, revisione e valutazione delle attività e degli obiettivi prefissati ed approvati. Il piano deve chiaramente indicare l'origine e la motivazione e in che tempi e modi intende essere applicato. Il responsabile deve periodicamente informare sullo stato dei lavori.

- **Controlli**: Ogni controllo ha un proprietario che ha la responsabilità per lo sviluppo, revisione e valutazione dello stesso. Ogni controllo adottato deve fare riferimento ad un requisito (ISO, regolamentazione, contratto etc) e deve chiaramente mitigare o trattare un rischio individuato. Gli assessment come ad esempio audit, checklist e i

relativi report scaturiti da queste attività sono considerati dei controlli per il processo di gestione della sicurezza informatica.

- **Assessment**: L'assessment è una attività di verifica volta a valutare la situazione o il setting attuale di un servizio, applicazione, tecnologia etc. L'assessment viene effettuato in maniera programmata oppure a seguito di una richiesta specifica (ad es. un incidente che ha richiesto un'investigazione più approfondita, oppure la richiesta di un cliente esterno).

- **Report**: il report viene sempre compilato a seguito di un assessment. Il report deve sempre definire lo scopo dell'attività, i valori che sono emersi dall'assessment, i risultati che ci si aspettava e ovviamente una comparazione (qualitativa o qualitativa) tra i valori attuali e quelli attesi. Il report deve anche dare una indicazione delle possibili azioni successive per mitigare situazioni di rischio.