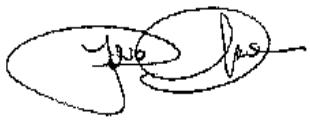
Procedura ISMS ISO 27001

P04-02 ISMS Politica del sistema

Revisioni

Revisione	Data	Autore	Motivazione
01	20/10/2022	M. Di Domenico	Prima emissione

Emesso	Controllato	Approvato
ISM	RAQ	AU
		

1 INTRODUZIONE

1.1 Presentazione della procedura

Il presente documento è stato redatto con l'obiettivo di fornire gli indirizzi e il supporto della direzione per l'istituzione, realizzazione, conduzione, monitoraggio, riesame, manutenzione e miglioramento dell'ISMS documentato nel contesto delle attività complessive istituzionali e dei rischi che IAD si trova ad affrontare.

Per la conformità alla Norma Internazionale ISO/IEC 27001 il processo utilizzato è basato sul modello **PDCA** (*Plan - Do - Check - Act*) illustrato in Figura 1.

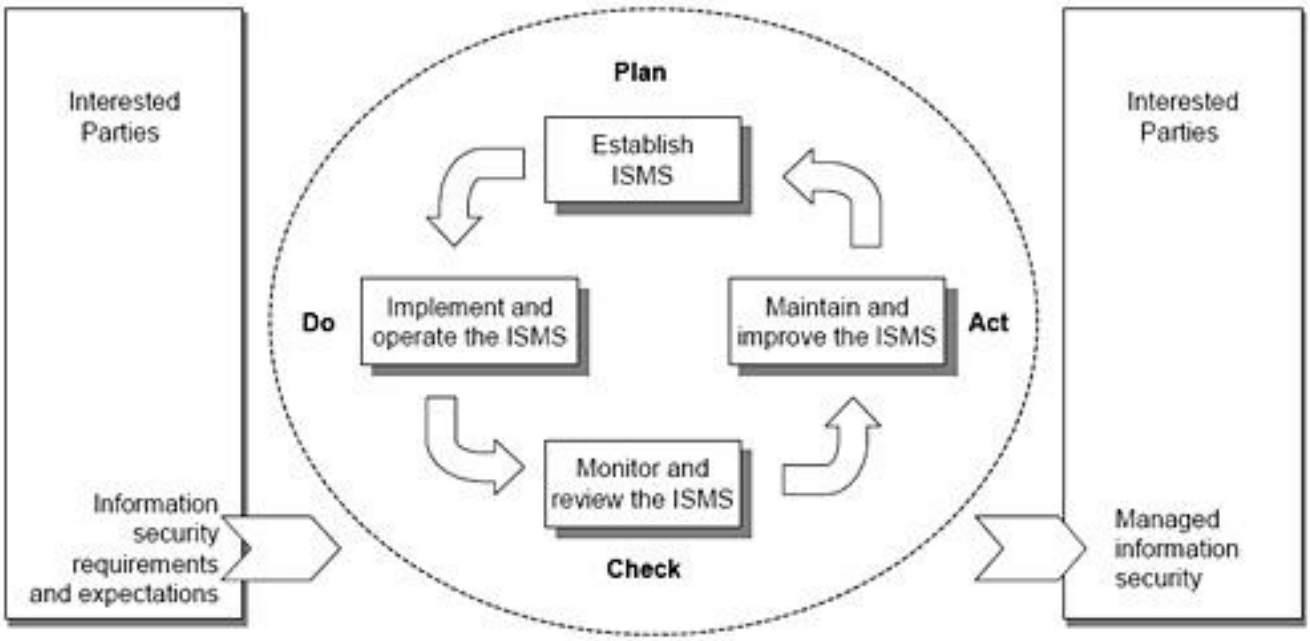


Figura 1 – Modello PDCA applicato ai processi del SGSI.

Plan *(Istituire il SGSI)*	Istituire la politica del SGSI, gli obiettivi, i processi e le procedure specifiche per gestire i rischi e migliorare la sicurezza delle informazioni al fine di produrre risultati coerenti con le politiche e gli obiettivi generali dell'organizzazione
DO *(Realizzare e condurre il SGSI)*	Applicare e rendere operativa la politica del SGSI, i controlli, i processi e le procedure
Check *(Monitorare e riesaminare il SGSI)*	Valutare e, dove applicabile, misurare le prestazioni del processo nei confronti della politica del SGSI, degli obiettivi e delle esperienze pratiche, quindi inoltrare i risultati alla direzione per il riesame
Act *(Manutenere e migliorare il SGSI)*	Intraprendere azioni correttive e preventive, basate sui risultati degli audit interni del SGSI, sul riesame da parte della direzione e su altre informazioni specifiche, al fine di ottenere un continuo miglioramento del SGSI

Tabella 1 – Definizione del modello PDCA

IAD ha già da anni implementato un sistema gestione della Qualità e il suo ISMS si integra con esso andando a individuare e definire i controlli per la sicurezza adeguati e proporzionati in grado di proteggere i beni informativi coinvolti nei processi.

1.2 Terminologia, sigle ed abbreviazioni

AU	Amministratore Unico
ISMS	Information Security Management System
ISM	Information Security Manager
RAQ	Responsabile Assicurazione Qualità
SGQ	Sistema Gestione Qualità
RRSK	Responsabile Risk Management
RAMM	Responsabile Amministrazione e Controllo
RACQ	Responsabile Acquisti (Approvvigionamento)
RRU	Responsabile Risorse Umane
RCOMM	Responsabile Commerciale
RDLY	Responsabile Delivery

RSI	Responsabile Sistemi Informativi
PM	Project Manager
SAMM	Segreteria Amministrativa
SCOMM	Segreteria Commerciale

1.3 Documenti di riferimento

I seguenti documenti di riferimento sono indispensabili per l'applicazione del presente documento.

Per i riferimenti non datati, vale l'ultima edizione del documento a cui si fa riferimento (compresi gli aggiornamenti).

1.3.1 Standard e normative

[Std. 1] ISO/IEC 27001 – 2013 e 2022

[Std. 2] ISO 31000 – 2018

1.3.2 Normative gestione dei dati personali

- Regolamento (UE) 2016/679 (GDPR)
- Trattamento dei dati nel rapport lavorativo
    - Deliberazione Garante 1/03/2007 n.13 "Linee guida del Garante per posta elettronica e internet" (G.U. n.58 del 10/03/2007)
    - Deliberazione Garante 23/11/2006 n.53 "Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro alle dipendenze di datori di lavoro privati
    - Provvedimento Garante 24 febbraio 2005 "'Fidelity card' e garanzie per i consumatori. Le regole del Garante per i programmi di fidelizzazione"
    - Videosorveglianza
    - Provvedimento in materia di videosorveglianza - 8 aprile 2010 (Gazzetta Ufficiale n. 99 del 29 aprile 2010)
    - Provvedimento Garante 29/04/2004 "Videosorveglianza - Provvedimento generale"

1.3.3 Normative Diritto di Autore

- Legge 22/04/1941 n.633 "Protezione del diritto d'autore e di altri diritti connessi al suo esercizio", e successive modifiche
- D.Lgs. 29/12/1992 n. 518 "Attuazione della direttiva 91/250/CEE relativa alla tutela giuridica dei programmi per elaboratore"

- Legge 18/08/2000, n. 248 "Nuove norme di tutela del diritto d'autore"

1.3.4 Documenti correlati

- P05.07.09.10-01 Leadership-Supporto-Valutazione Prestazioni-Miglioramento
- P08-03_Gestione Servizi Professionali sw
- P08-03_Progettazione e realizzazione progetti sw
- P08-05-05_Servizi di AM e post consegna
- IS20_ Inventory Asset per la sicurezza delle Informazioni
- IS12 Gestione Security
- IS01 _Gestione del rischio e continuità di business
- RSH_RuoloStakehoder
- GdR_GestionedeiRischi
- IAD_ProfiliProfessionali

1.4 Responsabilità

L'Information Security Manager dell'ISMS ha il compito di:

- Verificare la rispondenza ai requisiti della norma di riferimento ed alla Politica della Sicurezza definita dalla Direzione Aziendale;
- Verificare la congruità con i requisiti della norma di riferimento, con le Procedure, le guide e tutti i documenti dell'ISMS;
- Curare l'aggiornamento e la distribuzione di tutti i documenti costituenti l'ISMS.

Tutto il personale di IAD è chiamato a contribuire attivamente all'applicazione, all'aggiornamento e al miglioramento dell'ISMS.

1.5 Aggiornamento della documentazione ISMS

Le modifiche alle procedure e alle istruzioni possono essere proposte da tutti i destinatari dei rispettivi documenti. Gli aggiornamenti sono eseguiti dall'ISM con il supporto del RQA che ha il compito di gestione della documentazione. L'aggiornamento della documentazione segue le indicazioni riportate nel documento IS 07 Gestione Documenti.

1.6 Distribuzione della documentazione ISMS

I documenti del sistema ISMS sono distribuiti sempre in forma controllata. Per copia in forma controllata si intende che la copia del documento è identificata con un numero progressivo e registrata e mantenuta aggiornata.

1.7 Mansioni

I ruoli e le responsabilità sono riportati nell'istruzione di lavoro IS 12 "Gestione Security" par. 3.

In tale istruzione sono definite le principali responsabilità, l'autorità e i compiti dei Responsabili di funzione nell'ambito delle singole aree, con particolare riguardo a quelle che hanno rilevanza sulla sicurezza dei processi e dei servizi erogati.

Ogni responsabile di funzione ha inoltre analizzato, discusso e collaborato nello stabilire le responsabilità individuali di ogni singola attività di IAD.

2 POLITICA DEL SISTEMA

2.1 Obiettivi e scopo

Il presente documento illustra il contesto di riferimento ed i criteri secondo cui sono definiti i provvedimenti che IAD adotta come guida, nella realizzazione della propria missione aziendale, in tema di Sicurezza delle Informazioni finalizzata a preservare la Integrità, Disponibilità e Riservatezza delle informazioni trattate.

IAD adotta e diffonde ad ogni livello la presente politica, la quale viene anche applicata alle interfacce, individuando le Parti Interessate, siano esse interne o esterne con le quali IAD condivide processi di trattamento, di comunicazione e di elaborazione di informazioni.

La mission di IAD è supportare i Clienti nella protezione del proprio patrimonio informativo da rischi di intrusione e/o alterazione dei dati e delle applicazioni.

In tale ottica, IAD non poteva astenersi dal considerare l'esigenza di garantire la Sicurezza delle Informazioni, e ha quindi deciso di estendere il proprio sistema di gestione anche a tale aspetto. L'informazione rappresenta infatti un bene di primaria importanza, la cui protezione e sicurezza sono fondamentali per la buona riuscita dei servizi offerti.

IAD ha individuato la Norma Internazionale ISO/IEC 27001 quale strumento volontario adeguato alla Gestione della Sicurezza delle Informazioni, e si impegna al rispetto delle normative cogenti specifiche per la propria attività.

Scopo della politica per la Sicurezza delle Informazioni di IAD è di sottolineare il costante impegno a proteggere le informazioni trattate, consentendo simultaneamente:

- **Corretta gestione e protezione degli archivi dei dati**, sia su supporto cartaceo che elettronico, mediante valutazione preventiva di adeguatezza dei requisiti di sicurezza per ciascuna commessa, sicurezza dei processi mediante i quali sono trattate le informazioni e verifica dei provvedimenti adottati mediante riesame delle registrazioni indicate nel piano dei log, audit periodici, costante monitoraggio e utilizzo di appositi Key Performance Indicator.
- **Trasferimento di informazioni all'interno ed all'esterno del proprio ambito, mediante strumenti idonei a tutelare adeguatamente la riservatezza delle informazioni**.
- **Le strategie e le soluzioni per la protezione delle informazioni, nel rispetto delle leggi vigenti, come delle necessità contrattuali e di business richiedono il più ampio coinvolgimento e la responsabilità di ciascuno.**

Nella consapevolezza di quanto sia importante, il contributo di ciascun operatore coinvolto nei processi aziendali, oltre ai provvedimenti tecnici in senso stretto, la presente Politica intende quindi richiamare l'attenzione del Personale a un atteggiamento di collaborazione attiva e propositiva affinché quanto previsto sia mantenuto dinamicamente aggiornato efficace ed efficiente.

Principale obiettivo dell'adozione dell'ISMS è, quindi, quello di fornire all'organizzazione gli indirizzi, le prescrizioni e la documentazione di riferimento per quanto attiene la politica, gli obiettivi, la pianificazione, il controllo, l'assicurazione e il miglioramento della Sicurezza delle Informazioni, attraverso il pieno coinvolgimento del personale nel garantire la Sicurezza delle Informazioni trattate e specialmente quelle di proprietà dei Clienti, mediante la consapevole adozione di procedure a tutela della loro Integrità, Disponibilità e Riservatezza.

IAD ha definito un approccio alla valutazione dei rischi dell'organizzazione definendo una linea guida che garantisce una visibilità d'insieme sull'esposizione al rischio e sulle misure di sicurezza adottate. L'adozione di una metodologia di analisi contribuisce ad allineare le attività di gestione della Sicurezza delle Informazioni alle strategie di business aziendali, tramite un approccio strutturato, al fine di salvaguardare l'efficienza dei processi di business e di mantenere un elevato livello di confidenza sull'adeguatezza delle protezioni adottate.

La Politica è approvata dalla Direzione, e comunicata in modo appropriato a tutto il personale interessato. È inoltre riesaminata periodicamente per accertarne la continua idoneità nel corso del Riesame di Direzione.

La Politica per la Sicurezza delle Informazioni viene riesaminata a intervalli prestabiliti o in concomitanza di cambiamenti significativi per assicurare la sua perdurante idoneità, adeguatezza ed efficacia.

2.2 Campo di applicazione

Il perimetro di applicazione dell'ISMS che la Direzione ha identificato ed approvato è il seguente:

Progettazione, realizzazione, commercializzazione, installazione e manutenzione di soluzioni software personalizzate o prodotti software. Erogazione di servizi professionali e gestione applicativa in ambito IT

2.3 Analisi dei rischi

A fronte dell'Analisi dei Rischi, IAD ha predisposto procedure e istruzioni di lavoro documentate per la gestione del rischio relativo alle tipologie di incidenti possibili, incluso:

- Incidenti alla struttura (ad esempio: incendi, allagamenti, furto);
- Accessi non autorizzati;
- Malfunzionamento software o software corrotto.

Tali procedure riportano le modalità per gestire il rischio e da attuare in caso di emergenza. Nella istruzione "IS 13 Gestione degli Incidenti di sicurezza" sono indicate le modalità di gestione delle non conformità riscontrate e delle conseguenti azioni correttive, intraprese al fine di eliminare le cause che le hanno generate.

L'analisi dei rischi viene riportata nel documento "IAD-ISMS-AIRA", soggetto ad aggiornamento periodico.

Nell'analisi dei rischi sono applicati i controlli di sicurezza selezionati dalla Direzione. I controlli selezionati sono riportati nel documento "IAD SOAC".

2.4 Integrazione con il SGQ di IAD

IAD ha già da anni implementato un sistema gestione della Qualità. Il sistema ISMS quindi si integra con i processi del SGQ andandone a esplicitare i rischi per la sicurezza delle informazioni e selezionare i controlli efficaci nel garantire le caratteristiche di Integrità, Disponibilità e Riservatezza. Per questa ragione l'ISMS farà riferimento anche a procedure e istruzioni all'interno del SGQ di IAD e l'Information Security Manager è da intendersi coinvolto laddove siano presenti i temi della Sicurezza delle informazioni.

2.5 Ambito Fisico e Logico

L'ambito fisico del Sistema comprende:

- Amministrazione
- La struttura operativa
- Direzione

Site nella sede al secondo piano di Via Cristoforo Colombo 163 Roma.

Gli uffici sono protetti da un sistema antintrusione. Al di fuori dell'orario di lavoro, l'ingresso è chiuso. Le aree in cui possono essere custodite informazioni riservate/confidenziali o asset di importanza aziendale sono, quando non presidiate, normalmente chiuse a chiave.

Le altre sedi hanno uno scopo puramente operativo. Il personale si collega alla rete IAD passando per tutti i controlli di sicurezza previsti (Rif. Doc. IS03_Gestione HW e SW). I controlli di sicurezza applicati sono gestiti dalla sede di Via Cristoforo Colombo 163 (Roma).

L'obiettivo è quello di non conservare i file su un computer o un disco locale, bensì IAD ha optato per una più avanzata e affidabile soluzione di storage e backup in Cloud, che centralizzi sia la gestione delle autorizzazioni sia l'accesso ai dati. Per dettagli si veda Rif. Doc. IS03_Gestione HW e SW.

2.6 Ambito organizzativo

Le collaborazioni con parti terze (ad esempio: consulenti, fornitori, etc.) sono definite contrattualmente dalla Direzione. Il requisito di queste collaborazioni è trasmettere loro gli obiettivi dell'ISMS e allinearli con le sue procedure. A questo scopo sono predisposti i modelli per NDA (Non Disclosure Agreement, accordo di non divulgazione).

I fornitori sono inoltre sottoposti a valutazione come definito da SGQ di IAD.

Gli stakeholder individuati per l'ambito organizzativo sono riportati nel documento "P04-01-ISMS Contesto dell'organizzazione".

2.7 Privacy

Si veda il documento "IS 11 Gestione GDPR". In tale istruzione di lavoro vengono riportate le informazioni riguardanti la gestione in IAD in materia di trattamento dei dati personali.

2.8 Responsabilità, autorità, comunicazione

Tutti i processi aventi influenza sulla Sicurezza delle Informazioni sono regolati da procedure che definiscono le responsabilità nell'ambito del processo descritto.

La struttura organizzativa di IAD è rappresentata nell'organigramma aziendale aggiornato con data.

2.8.1 Rappresentante della Direzione

IAD ha nominato l'ISM (Information Security Manager), quale Rappresentante della Direzione per la Sicurezza delle Informazioni, e gli ha attribuito la responsabilità e l'autorità di assicurare che le prescrizioni del sistema per la Sicurezza delle Informazioni siano applicate e mantenute attive nel tempo.

2.8.2 Comunicazione e informazione

La comunicazione interna è gestita, nell'ambito di IAD, mediante:

- Riunioni;
- Incontri di formazione;
- Divulgazione di notizie concernenti l'assetto organizzativo dell'azienda e sue modifiche;
- Divulgazione di documentazione di specifico interesse;
- Diffusione di comunicazioni riguardanti i risultati dell'attività;
- Comunicazione scritta per invio ai singoli interessati di notizie relative ad argomenti di particolare importanza;
- Comunicazione alle funzioni interessate di Non Conformità, Azioni Preventive, Correttive e di Miglioramento;
- Impiego della rete intranet per la diffusione di notizie/documenti/comunicazioni di carattere operativo;

Ciascun responsabile gestisce, nell'ambito del proprio processo, le informazioni di proprio interesse ed è sensibilizzato a trasferire alle altre funzioni, e alla Direzione, le informazioni di comune interesse.

Le fonti d'informazione esterne sono considerate:

- La stampa e pubblicazioni specializzate;
- La rete internet;
- Seminari e convegni;
- Corsi di formazione;

2.9 Risorse

2.9.1 Personale

La Direzione, nell'ambito dei propri obiettivi attuali e di sviluppo, individua le competenze necessarie per il conseguimento dei risultati prefissati. In particolare:

- Definisce le regole di selezione, formazione continua e pianificazione delle carriere;
- Definisce i requisiti minimi di valutazione per le assunzioni di ruolo;
- Individua le responsabilità e autorità per le attività operative;
- Individua gli obiettivi individuali di gruppo, valutandone i risultati;
- Predispone l'addestramento necessario per tale attività;
- Valuta l'efficacia dell'addestramento fornitogli e del lavoro di gruppo.

IAD considera la formazione strumento essenziale per la crescita professionale dei dipendenti e per il miglioramento costante della qualità dei servizi erogati.

Sono stati definiti i criteri e i modi per individuare le necessità di formazione e addestramento dei dipendenti. Tutta l'attività formativa sull'ISMS è opportunamente registrata e pianificata.

2.9.2 Infrastrutture

IAD individua, fornisce e mantiene le infrastrutture necessarie per assicurare la conformità alle esigenze del personale e alla normativa ISO/IEC 27001 vigente sulla sicurezza, adeguata disponibilità di apparecchiature e software, servizi di supporto.

Per la gestione dell'infrastruttura tecnologica, sono previste e pianificate attività preventive/manutentive" quali, ad esempio:

- Installazione e aggiornamento periodico di programmi per protezione, individuazione ed eliminazione di virus;
- Installazione e aggiornamento periodico di sistemi operativi e programmi di supporto allo sviluppo;
- Manutenzione della Rete Intranet/Internet;
- Backup/Restore dei server e delle postazioni di lavoro.