0.7 Requisiti della norma e applicazione da parte dell'organizzazione

Nei paragrafi che seguono, l'organizzazione ha provveduto ad illustrare, in maniera sintetica e schematica, la modalità con cui adempie ai requisiti della ISO 27001:2017. Ciascun paragrafo è dedicato ad un punto preciso della Norma così da fornire, a tutte le persone interessate, un quadro chiaro del funzionamento del sistema di gestione di sicurezza delle informazioni.

STRUTTURA DELLA NORMA E SEZIONI DEL MANUALE	
1	Scopo e campo di applicazione
2	Riferimenti normativi
3	Termini e definizioni
4	Contesto
5	Leadership
6	Pianificazione
7	Supporto
8	Attività operative
9	Prestazioni
10	Miglioramento

I contenuti del manuale privilegiano l'informazione di sintesi. Ciascun punto, tuttavia, rimanda gli approfondimenti ad altri documenti quali procedure e modulistica dello stesso sistema. Eventuali incomprensioni o necessità di chiarimenti possono essere riportate al responsabile del sistema di gestione delle informazioni che è:

dott. Mario Rossi
responsabile_sistema@organizzazione.it

4 Contesto

Comprendere le necessità e le aspettative delle parti interessate

Monitorare il contesto significa anche identificare continuamente le parti interessate alla protezione delle informazioni e le loro specifiche esigenze di riservatezza, integrità e disponibilità dei dati. Grazie alla procedura **PROC-400 - Monitoraggio del contesto,** l'organizzazione tiene sempre sotto controllo le esigenze di coloro interessati alla protezione delle informazioni, potendo così fornire a costoro le giuste garanzie a riguardo dei controlli impiegati per la protezione delle informazioni.

L'organizzazione, grazie all'applicazione della procedura **PROC-400 - Monitoraggio del contesto**, esercita un'importante attività di osservazione del **mondo interno ed esterno** ad essa creando dei momenti di condivisione formale delle informazioni durante i quali, i soggetti partecipanti, individuano e riesaminano fattori influenti, parti interessate ed esigenze delle parti interessate.

Campo di applicazione del sistema di gestione

In questa sezione del manuale l'organizzazione ha provveduto a stabilire il campo di applicazione del sistema di gestione per la sicurezza delle informazioni.

Oggetto della sicurezza delle informazioni:

- Dati riguardanti l'identità, il funzionamento e la struttura del soggetto o dei soggetti committenti e fornitori
- Dati riguardanti la modalità con cui l'organizzazione provvede alle attività di analisi statistiche es: data mining

Processi di trattamento delle informazioni: Processi "primari" (o alternativamente chiamati anche processi operativi)

L'organizzazione svolge la propria attività di consulenza per il data mining attraverso processi operativi che vanno dalla raccolta iniziale dei dati del committente fino alla fornitura - a questi - dei risultati delle analisi. Tali processi che rientrano nel campo di applicazione del presente sistema di gestione sono i seguenti e sono riportati, con la loro denominazione originaria, dalle corrispondenti procedure redatte, applicate e conservate in organizzazione:

- Requisiti
- Progettazione
- Outsourcing
- Produzione
- Preservazione
- Controllo output non conformi

5 Leadership

Politica

La Politica per la sicurezza delle informazioni è stata definita dalla Leadership dell'organizzazione, in modo tale:

- Da risultare appropriata alle finalità dell'organizzazione
- Da costituire un quadro di riferimento per fissare gli obiettivi di sicurezza
- Da includere l'impegno a rispettare i requisiti applicabili e attinenti alla sicurezza delle informazioni
- Da mantenere l'impegno per il miglioramento continuo del sistema di gestione

La Politica per la sicurezza delle informazioni è resa disponibile come informazione documentata, è comunicata all'interno dell'organizzazione, è resa disponibile per le parti interessate.

E ancora:

- La politica è accessibile sul sito internet istituzionale dell'organizzazione
- Viene comunicata al personale aziendale attraverso l'invio tramite mail
- È affissa nelle bacheche dell'organizzazione da poter essere visibile al personale e agli eventuali visitatori

L'organizzazione adotta due livelli di politica per la sicurezza delle informazioni:

- Il livello più alto, livello A, documenta la politica generale all'interno del **MOD-520 - Politica per la sicurezza delle informazioni**.
- Il livello inferiore, livello B, documenta le politiche specifiche per argomento. Le politiche specifiche sono riportate nelle procedure in riferimento a ciascun controllo dell'Annex A per le quali sono previste. Esse sono:
  - Politica per l'impiego dei dispositivi portatili
  - Politica per il telelavoro
  - Politica per il controllo degli access
  - Politica dell'impiego di controlli crittografici
  - Politica di schermo e scrivania puliti
  - Politica di backup
  - Politica per il trasferimento delle informazioni
  - Politica per lo sviluppo sicuro
  - Politica per la sicurezza nei rapporti con i fornitori

Il termine *policy* utilizzato nell'accezione della norma, tradotto in italiano, significa "regola" o "regole". L'organizzazione, tuttavia, ha inteso il termine *policy* in senso più ampio, sviluppando delle vere e proprie politiche in senso generale rispetto all'argomento, riservando alle procedure il compito di spiegare le singole "regole" che disciplinano il funzionamento dei processi di sicurezza.

6 Pianificazione

Pianificazione

In relazione ai rischi e alla loro entità, l'organizzazione ha redatto il Piano di sicurezza delle informazioni riportato nel modulo **MOD-610-B- Piano di sicurezza delle informazioni** con il quale ha provveduto ad attivare i controlli per la sicurezza delle informazioni. Il piano è uno dei documenti fondamentali del sistema di gestione poiché spiega come l'organizzazione intende proteggere le informazioni e rassicura i terzi circa le modalità con cui l'organizzazione applica i controlli di sicurezza alle informazioni elaborate e trattate.

I controlli di sicurezza nelle procedure gestionali

I controlli di sicurezza attivati dall'organizzazione sono quelli indicati dall'Annex A della Norma ISO 27001:2017 (si tratta di un allegato della norma in cui è presente un elenco di misure da adottare in corrispondenza di determinate circostanze quali ad esempio la protezione fisica delle strutture, il controllo di accesso alla rete, il backup delle informazioni etc.).

Questi controlli sono stati integrati all'interno delle procedure gestionali e cioè quelle procedure che disciplinano l'intero funzionamento dell'azienda attraverso i suoi processi "primari" definiti anche come "operativi" quali: progettazione, produzione, etc. e i processi di supporto quali invece l'analisi del contesto, la pianificazione, il riesame di direzione, etc.).

L'integrazione è stata effettuata come segue nell'esempio. Il testo è tratto dalla procedura gestionale **PROC-710 - Gestione degli asset**, nella quale, nelle attività gestionali sono stati integrati i controlli di sicurezza dell'Annex A, con il loro numero.

[controllo 8.1.4] Restituzione degli asset
Tutto il personale e gli utenti di parti esterne devono restituire tutti gli asset dell'organizzazione in loro possesso al termine del periodo di impiego, del contratto o dell'accordo stipulato.

I contratti di lavoro dell'organizzazione prevedono espressamente a carico del personale la restituzione di tutti gli asset dell'organizzazione in loro possesso al termine del periodo di impiego, del contratto o dell'accordo stipulato.

La restituzione viene registrata all'interno del modulo MOD-710-M- Inventario degli asset. La registrazione dell'avvenuta restituzione consiste nell'assegnazione, in una determinata data, ad un altro responsabile oppure all'organizzazione stessa (RGSI) che la tiene in carico in attesa di una nuova assegnazione.

[controllo 8.3.1] Gestione dei supporti rimovibili
Devono essere sviluppate procedure per il trattamento dei supporti rimovibili in base allo schema di classificazione adottato dall'organizzazione

L'organizzazione, all'interno del modulo MOD-710-M- Inventario degli asset ha individuato un campo con cui stabilire se l'asset è rimovibile. Tale "rimovibilità", associata comunemente ai soli dispositivi di memoria (es: chiavette USB, Hard Disk portatile, etc.), viene estesa a tutti gli asset fisici che possono essere trasportati (magari trascinati o trafugati) al di fuori dell'organizzazione

6 Pianificazione

I controlli nelle procedure di sicurezza

Per alcuni controlli presenti all'interno dell'Annex A della norma è stato necessario redigere delle procedure a parte, che a differenza delle altre (procedure gestionali) si configurano come "procedure di sicurezza". Esse, infatti, non disciplinano il funzionamento dell'organizzazione ma disciplinano l'attuazione di controlli di sicurezza per le informazioni.

Queste procedure che recano il prefisso PSI (procedura di sicurezza delle informazioni) riportano, accanto all'acronimo anche il numero del controllo con il quale esso è identificato nell'Annex A della norma. Esse sono:

- PSI-06 – Telelavoro e sicurezza delle informazioni
- PSI-09 – Controllo degli accessi
- PSI-10 – Crittografia
- PSI-11 – Sicurezza fisica e ambientale delle informazioni
- PSI-12 – Sicurezza operativa
- PSI-13 – Sicurezza delle comunicazioni
- PSI-14 – Acquisizione, sviluppo e manutenzione dei sistemi
- PSI-16 – Gestione degli incidenti relativi alla sicurezza delle informazioni
- PSI-17 – Gestione continuità operativa della sicurezza delle informazioni
- PSI-18 – Conformità

Gli obiettivi dell'organizzazione

La finalità strategica dell'organizzazione, in riferimento al sistema di gestione in questione, è la protezione delle informazioni dal rischio di perdita di riservatezza, integrità e disponibilità.

L'organizzazione, nell'intento di focalizzare gli sforzi per il perseguimento di tale finalità verso traguardi specifici e misurabili, ha stabilito degli obiettivi di sicurezza, misurati attraverso l'indice di sicurezza, in riferimento a:

- Sicurezza risorse umane
- Sicurezza rete e comunicazioni
- Sicurezza nella qualità della formazione
- Sicurezza nel software
- Sicurezza nei dispositivi di elaborazione
- Sicurezza della sede e degli archivi
- Sicurezza degli impianti e dei dispositivi di sicurezza

Quando si fa riferimento alla "sicurezza risorse umane" non ci si riferisce alla sicurezza degli individui ma alla sicurezza delle informazioni rispetto ai rischi che potrebbero provenire dalle persone.

Persone e competenze

Data l'influenza che le risorse umane possono esercitare sulla sicurezza delle informazioni, l'organizzazione ha provveduto a redigere una procedura che integra i controlli di sicurezza riservati al personale (dall'Annex A) attraverso una serie di passaggi per i quali essa deve:

- Determinare le competenze necessarie per le risorse umane che svolgono attività lavorative sotto il controllo dell'organizzazione e che influenzano le prestazioni e l'efficacia del SGSI
- Stabilire dei requisiti di affidabilità delle persone che devono trattare informazioni sensibili
- Assicurare che le risorse umane siano affidabili e competenti sulla base di istruzione, formazione, o esperienza appropriate
- Intraprendere azioni per acquisire l'affidabilità e le necessarie competenze e valutare l'efficacia delle azioni intraprese
- Conservare appropriate informazioni documentate quale evidenza dell'affidabilità e delle competenze

La procedura stabilisce che, a seguito della ricognizione che permette di comprendere di quali figure essa ha bisogno, venga effettuata una accurata selezione di candidati che posseggano specifici requisiti relativi a:

- Titolo di studio
- Esperienze
- Conoscenze pregresse
- Competenza
- Consapevolezza

L'assunzione del personale, in tale procedura, è una fase delicata in cui vengono applicati dei controlli di sicurezza relativi agli aspetti contrattuali per i quali si assumono specifici impegni relativi alla riservatezza e all'utilizzo degli asset resi disponibili dall'organizzazione.

Il personale, in relazione al proprio ruolo, viene costantemente formato e reso sensibile ai rischi per la sicurezza delle informazioni. Le applicazioni gestionali correlate alla procedura **PROC-720 - Persone e competenze** permettono di tenere sotto controllo le attività formative e la qualità della formazione svolta. L'organizzazione, infatti, è consapevole che la formazione e la sensibilizzazione delle risorse umane costituiscano le misure principali per la prevenzione dei rischi.

Ancorché il sistema di gestione sia concepito perfettamente con tutti i suoi controlli, esso potrebbe essere reso vano dal comportamento di persone che aggirano consapevolmente le regole stabilite allo scopo di arrecare danno. A tale proposito la procedura stabilisce il funzionamento del **processo disciplinare** a cui potrebbe essere sottoposto il personale che infrange le regole.

8 Attività operative

Il punto 8 della Norma ISO 27001:2017 è stato gestito dall'organizzazione con l'intento di tracciare i processi operativi in tutte le loro fasi per tenere sotto controllo i rischi che sono presenti in tutte quelle attività che relazionano l'organizzazione con il cliente allo scopo di rendere a questi il prodotto/servizio che ha richiesto all'organizzazione.

L'organizzazione nella sua attività di business di fatto vende servizi di analisi dati. I processi operativi (definiti anche come primari) sono quelli che partono dalla raccolta dei requisiti che il cliente determina per la richiesta del proprio prodotto servizio fino alla produzione effettiva del prodotto servizio e al suo controllo in fase di rilascio.

Per favorire l'allineamento con altri sistemi di gestione presenti e futuri nell'organizzazione, il punto 8 della norma è stato sviluppato simulando (nella sola definizione della denominazione dei processi) una sorta di parallelismo tra i requisiti della ISO 9001 relativa alla gestione per la qualità e i processi operativi dell'organizzazione.

Alle procedure che disciplinano tali processi infatti sono state attribuite denominazioni che rievocano la sequenza delle attività operative presentate dalla ISO 9001.

L'opportunità di tale parallelismo che, come si noterà dall'applicazione effettiva dei documenti al sistema, semplificherà la comprensione dell'intero processo produttivo, è reso possibile dal fatto che la ISO 27001 e la ISO 9001 hanno la medesima struttura (High Level Structure) concepita dagli enti di normazione proprio per facilitare la comunicazione tra i sistemi di gestione differenti e coesistenti.

I processi operativi (primari) disciplinati dalle corrispondenti procedure sono i seguenti:

- PROC-812 – Requisiti
- PROC-813 – Progettazione
- PROC-814 – Outsourcing
- PROC-815 – Produzione
- PROC-816 – Preservazione
- PROC-817 - Controllo output non conformi

All'interno di ciascuna procedura sono stati integrati i controlli riportati dall'Annex A della ISO 27001:2017.

Valutazione delle prestazioni

Gli audit

L'organizzazione ha predisposto la procedura con cui effettua gli audit relativi alla conformità:

- Del sistema di gestione ai requisiti della norma ISO 27001:2017
- Delle procedure ai controlli stabiliti dall'annex A della norma
- Del comportamento delle persone alle prescrizioni contenute nelle procedure

La procedura **PROC-920 - Audit Interni** disciplina tutte le fasi delle attività di auditing quali:

- Pianificazione
- Preparazione
- Esecuzione
- Registrazione
- Chiusura
- Archiviazione
- Monitoraggio audit

Anche il processo di audit è tenuto sotto controllo dal punto di vista statistico dalle applicazioni gestionali. In questo caso il processo è monitorato, nel suo indice di sicurezza, attraverso il modulo in Excel **MOD-920-E-Monitoraggio auditing** che rileva automaticamente il livello di sicurezza in relazione alla modalità con cui l'organizzazione gestisce le non conformità e ne previene il ripetersi.

Il riesame di direzione

L'organizzazione, per assicurare che la direzione del sistema di gestione sia sempre orientata all'obiettivo strategico e non subisca derive verso momenti o situazioni di stallo, di inattività o di inefficienza, organizza attività di riesame periodicamente.

Alle riunioni di riesame di direzione, così come stabilito dalla procedura che ne disciplina il funzionamento **PROC-930 - Riesame di direzione**, partecipano l'alta direzione, i responsabili di processo (RDP) secondo le rispettive competenze ed il personale impiegato nella sicurezza delle informazioni.

10 Miglioramento

L'organizzazione provvede a rimuovere e prevenire qualunque ostacolo possa impedire la protezione delle informazioni o comprometterne la sicurezza. A tale scopo, quando rileva una non conformità che si è manifesta attraverso un comportamento intenzionale o ascrivibile alla distrazione procede con un esame approfondito della non conformità.

La procedura **PROC-1010 - Non conformità e azioni correttive** focalizza l'attenzione sull'analisi delle cause della non conformità e arriva a determinare i criteri per elaborare le azioni correttive che possano:

- Rimuovere gli effetti indesiderati della non conformità
- Prevenire che tale non conformità si ripresenti nel medesimo contesto o in altre circostanze

Le fasi illustrate nella procedura sono le seguenti:

- Classificazione della non conformità
- Rilevazione della non conformità
- Registrazione ed analisi della non conformità
- Determinazione dell'azione correttiva
- Attuazione dell'azione correttiva e verifica

PROC-1020 - Miglioramento continuo

Per tale punto della norma, l'organizzazione ha redatto la procedura dedicata al miglioramento continuo delle performance di sicurezza e di efficienza e di efficacia del sistema di gestione anche in senso più ampio. In tal senso l'organizzazione ha avviato una sorta di ufficio "ricerca & sviluppo" che ha identificato in un gruppo di miglioramento costituito da alcuni RDP (responsabili di processo) e altro personale dedicato alla sicurezza delle informazioni.

Come spiega nel dettaglio la procedura, al Gruppo di miglioramento è affidata la "missione" di analizzare i risultati del sistema di gestione per la sicurezza delle informazioni ed elaborare una strategia di miglioramento.

La strategia di miglioramento contenuta nel modulo **MOD-1020-A Strategia di miglioramento** viene presentata dal gruppo di miglioramento dall'alta direzione in occasione del riesame di direzione. La presentazione avviene in maniera ufficiale e, a seconda delle opportunità, avviene alla presenza dei soci finanziatori dell'organizzazione e alla presenza di tutte le parti interessate.

La strategia verrà resa operativa ed implementata sotto la guida dell'alta direzione da tutti i soggetti coinvolti ed indicati nella relativa documentazione.