

Kit Software Documentale Sistema di Gestione Sicurezza delle Informazioni, CyberSecurity e Protezione della Privacy ISO 27001:2024 | Aggiornato AMD-1 2024

Questo PDF contiene un esempio dei materiali Winple. Per verificare la versione, i contenuti completi, gli altri dimostrativi e la disponibilità, visita la scheda del prodotto.

APRI LA SCHEDA DEL PRODOTTO



www.wingle.it/kit-documentale-sicurezza-informazioni-iso-27001-2024/



INTRODUZIONE

QUAL È LO SCOPO DEL PRESENTE MANUALE

Lo scopo del presente manuale del sistema di gestione è quello di costituire una guida per:

- La comprensione degli elementi costitutivi del sistema di gestione
- La consapevolezza del funzionamento dei suoi processi verso lo scopo
- L'orientamento nei documenti di sistema e nella loro esatta funzione

Il manuale è stato redatto in maniera puntuale e ordinata per costituire un documento ufficiale di cui abbiamo riportato i principali destinatari e le corrispondenti funzioni:

DESTINATARI DEL MANUALE	FUNZIONE ASSOLTA DAL MANUALE
Organismo di certificazione	Rendicontare la conformità a tutti i requisiti della Norma ISO 27001:2024
	Fornire il riscontro documentale dell'applicazione dei requisiti della Norma ISO 2700:2024
	Dichiarare e dimostrare l'applicazione dei controlli dell'Annex A della ISO 27001:2024
Consulenti e manager	Disporre del controllo e della visione dell'intero sistema di gestione all'interno di un unico documento principale
	Disporre di un unico documento "master" che illustra sequenza e interazioni di tutti i processi che perseguono lo scopo del sistema
Formatori dell'organizzazione	Eseguire la formazione al personale: ▪ Sui processi di business e di sistema ▪ Sui processi di sicurezza ▪ Sulle regole e i criteri da rispettare ▪ Sulla documentazione da impiegare
Ispettori e pubblici ufficiali e committenti/clienti	▪ Esaminare la conformità alla norma ▪ Verificare l'attuazione dei requisiti previsti dal capitolato di gara ▪ Valutare l'idoneità del sistema per la sicurezza delle informazioni in fase di istruttoria di gara
Personale e parti interessate	▪ Comprendere e rispettare il funzionamento del sistema di gestione



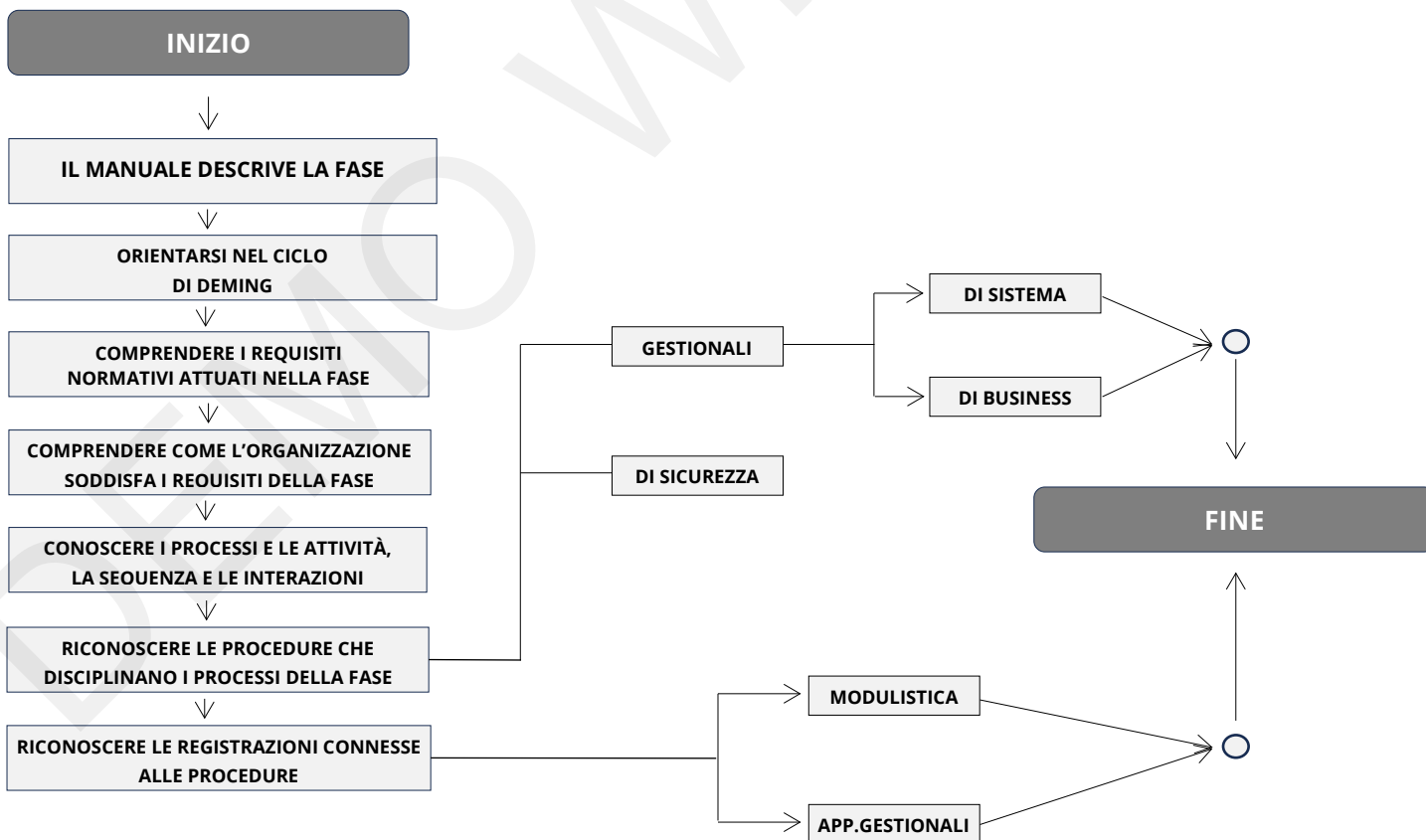
INTRODUZIONE

COME USARE EFFICACEMENTE IL MANUALE

Per comprendere, sviluppare e attuare il Sistema di gestione delle informazioni, la funzione di GUIDA del presente manuale procede nella seguente maniera:

1. Raggruppa tutti i requisiti della Norma 27001 nelle fasi del ciclo di Deming (PLAN, DO, CHECK E ACT) per dare un ordine sequenziale allo sviluppo del lavoro
2. Di ciascuna fase (PLAN, DO, CHECK E ACT):
 - a. Fornisce una descrizione generale di come l'organizzazione affronta la specifica fase
 - b. Stabilisce quali sono i processi del sistema appartenenti alla fase e le procedure che li disciplinano
 - c. Elenca le attività eseguite nei processi e le descrive
 - d. Indica le registrazioni e cioè le informazioni documentate che documentano le informazioni trattate nei processi

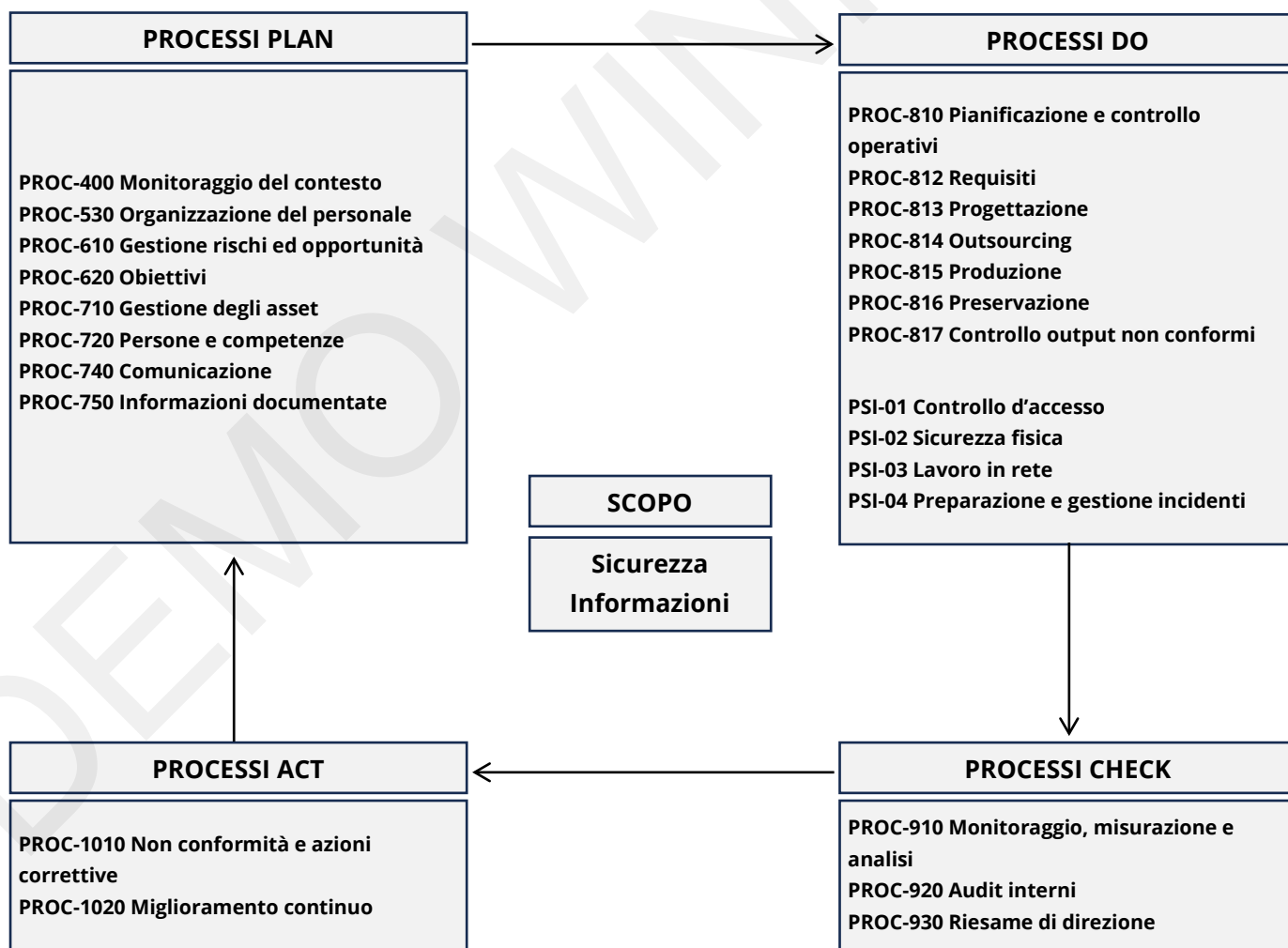
L'utente del manuale è invitato ad osservare le seguenti istruzioni per poter ottimizzare i risultati connessi alla comprensione dei contenuti.



**L'IMPIANTO PROGETTUALE DEL SISTEMA DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI****L'ADOZIONE DEL CICLO DI DEMING COME STRATEGIA DI SVILUPPO DEL SISTEMA**

Il sistema di gestione persegue lo scopo generale della sicurezza delle informazioni attraverso una sequenza di azioni che, disciplinate dalle procedure, si ripetono ciclicamente. Queste attività appartengono rispettivamente alle 4 fasi del ciclo di DEMING (PLAN, DO, CHECK, ACT).

- PLAN: Pianifica cosa fare
- DO: Esegui quanto hai pianificato
- CHECK: Verifica che quanto hai eseguito sia conforme a quanto pianificato
- DO: Intervieni in caso di scostamento





FASE PLAN: REQUISITI NORMATIVI ATTUATI NELLA FASE

La nostra organizzazione, in relazione alle scelte di funzionamento del sistema, ha considerato i seguenti requisiti normativi per sviluppare i processi connessi alle attività (PLAN) di pianificazione del ciclo di DEMING.

PUNTI NORMA ISO 27001:2024	PARTE PLAN
	REQUISITI NORMATIVI DEL SISTEMA DI GESTIONE
CONTESTO	4 Contesto dell'organizzazione
	4.1 Comprendere l'organizzazione e il suo contesto
	4.2 Comprendere le esigenze e le aspettative delle parti interessate
	4.3 Determinazione dell'ambito di applicazione del sistema di gestione della sicurezza delle informazioni
	4.4 Sistema di gestione della sicurezza delle informazioni
LEADERSHIP	5 Leadership
	5.1 Leadership e impegno
	5.2 Politica
	5.3 Ruoli, responsabilità e autorità dell'organizzazione
PIANIFICAZIONE	6 Pianificazione
	6.1 Azioni per affrontare i rischi e le opportunità
	6.1.1 Generalità
	6.1.2 Valutazione dei rischi per la sicurezza delle informazioni
	6.1.3 Trattamento dei rischi per la sicurezza delle informazioni
	6.2 Obiettivi di sicurezza delle informazioni e pianificazione per raggiungerli
SUPPORTO	7 Supporto
	7.1 Risorse
	7.2 Competenza
	7.3 Consapevolezza
	7.4 Comunicazione
	7.5 Informazioni documentate
	7.5.1 Generalità
	7.5.2 Creazione e aggiornamento
	7.5.3 Controllo delle informazioni documentate



FASE PLAN: COME L'ORGANIZZAZIONE SODDISFA I REQUISITI DELLA FASE

LA PROCEDURA MONITORAGGIO DEL CONTESTO

L'organizzazione risponde a tali requisiti attraverso l'istituzione della procedura **PROC-400 Monitoraggio del contesto**.

Mediante l'applicazione di tale procedura l'organizzazione ha compreso che i fattori che hanno una maggiore influenza reale o potenziale sull'effettivo raggiungimento dello scopo siano i seguenti:

- Consapevolezza dei rischi da parte delle persone
- Consapevolezza dei rischi da parte dell'alta direzione
- Formazione delle persone nell'ambito della sicurezza delle informazioni e la sicurezza informatica
- Evoluzione tecnologica del settore della sicurezza nella gestione delle informazioni
- Adeguatezza tecnologica dei dispositivi per la protezione fisica e logica dei dati
- Budget disponibile da impiegare in investimenti per la sicurezza delle informazioni

I soggetti che l'organizzazione invece ha individuato tra coloro che hanno una maggiore influenza sull'effettivo raggiungimento dello scopo della protezione delle informazioni sono le seguenti parti interessate:

- Clienti
- Compagine societaria/proprietaria dell'organizzazione
- Investitori
- Persone dell'organizzazione

Identificare tutte le "variabili indipendenti" che incidono o possono incidere sulla "variabile scopo" permette all'organizzazione di esaminare come queste esercitano questa influenza e come, attraverso la pianificazione, tali variabili possono essere controllate in favore dello scopo.

Per eseguire tale attività di monitoraggio di tipo "legislativo" del contesto, l'organizzazione impiega l'allegato **ALL-A Delitti informatici e trattamento illecito dei dati**, presente nella cartella di sistema "ALLEGATI",

L'Art.24-bis del D.Lgs.n.231/01, in relazione alla responsabilità amministrativa dell'organizzazione, individua i reati presupposto connessi ai delitti informatici e al trattamento illecito dei dati.

L'organizzazione, con tale documento, comunica al proprio staff dirigenziale, a propri dipendenti, ai consulenti e alle parti interessate, quali sono le fattispecie di reato previste all' Art.24-bis del D.Lgs.n.231/01, in relazione alle quali i comportamenti e le condotte poste in essere dalle persone si configurerebbero come reato.

**FASE PLAN: COME L'ORGANIZZAZIONE SODDISFA I REQUISITI DELLA FASE****L'INDIVIDUAZIONE, LA VALUTAZIONE E IL TRATTAMENTO DEL RISCHIO PER LE INFORMAZIONI**

La procedura **PROC-610 Gestione rischi ed opportunità** in relazione ai rischi per le informazioni da affrontare stabilisce una sequenza esatta di azioni da compiere:

- Identificazione dei processi
- Identificazione della categoria del processo (Processo di business, Processo di sicurezza)
- Per ciascuna categoria di processo:
 - Stabilire quali informazioni sono a rischio
 - Individuare quali sono i documenti che contengono le informazioni a rischio
 - Identificare i ruoli aziendali attivi (persone che operano nei processi)
 - Individuare le minacce derivanti dalle persone
 - Individuare e valutare i rischi ascrivibili al comportamento delle persone
 - Individuare le minacce fisiche che possono compromettere gli asset impiegati nei processi
 - Individuare e valutare i rischi ascrivibili alle minacce fisiche
- Individuare i controlli necessari a riportare i rischi ad un livello accettabile
- Integrare i controlli nei processi aziendali

L'organizzazione compie queste azioni che rappresentano la modalità ordinaria con la quale l'organizzazione provvede a gestire il rischio.

La modalità straordinaria, che invece vedremo in seguito, è gestita dalla procedura **PSI-04 Preparazione e gestione incidenti**.

La procedura **PROC-610 Gestione rischi ed opportunità** impone all'organizzazione di eseguire sistematicamente le azioni di pianificazione e aggiornare due documenti molto importanti:

- **MOD-610-A Identificazione e valutazione del rischio**
- **MOD-610-B Piano di sicurezza delle informazioni**

L'organizzazione ha sintetizzato in tre eventi fondamentali il rischio di sicurezza delle informazioni e cioè:

- Perdita di riservatezza
- Perdita di integrità
- Perdita di disponibilità

Nel modulo **MOD-610-A Identificazione e valutazione del rischio**, in relazione a ciascun processo esaminato, sono state individuate anche le minacce. Esse sono anche definite pericoli poiché rappresentano la fonte del rischio oppure l'occasione per la quale il rischio insorge, oppure ancora, aumenta la sua probabilità o il danno che provoca.



FASE PLAN: COME L'ORGANIZZAZIONE SODDISFA I REQUISITI DELLA FASE

OBIETTIVI DI SICUREZZA E PIANIFICAZIONE

Tutta la fase PLAN del sistema termina, e si sintetizza, nella determinazione degli obiettivi di sicurezza per le informazioni, specifici e misurabili, che il sistema deve raggiungere per poter affermare di aver conseguito lo scopo.

Riassumendo i processi della fase PLAN attraverso le corrispondenti procedure:

- La procedura **PROC-400 Monitoraggio del contesto** permette di conoscere cosa influenza il perseguimento dello scopo del sistema di gestione
- La procedura **PROC-530 Organizzazione del personale** permette di stabilire impegni, ruoli e responsabilità per gestire il contesto e perseguire lo scopo secondo i principi stabiliti nella Politica
- La procedura **PROC-610 Gestione rischi ed opportunità** consente di individuare le incertezze che è necessario affrontare con azioni di pianificazione e permette di stimare il valore del rischio a cui sono sottoposte le informazioni a cui l'organizzazione risponde con l'applicazione dei controlli del **MOD-610-B Piano di sicurezza delle informazioni**
- La procedura **PROC-620 Obiettivi**, per concludere, determina dei risultati specifici e misurabili, in termini di sicurezza, che affrontando il contesto e le sue incertezze, l'organizzazione deve raggiungere per dare compimento "oggettivo" al raggiungimento dello scopo.

Lo scopo dell'organizzazione ha la seguente enunciazione, breve e semplice, da scrivere, pronunciare, ricordare, immaginare ed ispirare, in generale i comportamenti:

"PROTEGGERE LA SICUREZZA DELLE INFORMAZIONI"

Con la determinazione degli obiettivi di sicurezza, l'organizzazione specifica i risultati attesi connessi allo scopo.

OBIETTIVO	RISULTATO	SCADENZA	RISORSE	RESPONSABILE
Sicurezza delle risorse umane	Indice sicurezza = 5	31/12/2024	2.100 €	RGSI
Sicurezza della rete e delle comunicazioni	Indice sicurezza = 5	31/12/2024	2.100 €	RGSI
Sicurezza della qualità della formazione	Indice sicurezza = 5	31/12/2024	2.100 €	RGSI
Sicurezza del software	Indice sicurezza = 5	31/12/2024	2.100 €	RGSI
Sicurezza dei dispositivi di elaborazione	Indice sicurezza = 5	31/12/2024	2.100 €	RGSI
Sicurezza della sede e degli archivi	Indice sicurezza = 5	31/12/2024	3.100 €	RGSI
Sicurezza degli impianti e dei dispositivi di sicurezza	Indice sicurezza = 5	31/12/2024	3.100 €	RGSI



FASE PLAN: COME L'ORGANIZZAZIONE SODDISFA I REQUISITI DELLA FASE

GLI ASSET DELL'ORGANIZZAZIONE E LA LORO SICUREZZA

Gli asset dell'organizzazione consistono in "Informazioni" e supporti di qualunque natura destinati a trattarle e/o a proteggerle. Di seguito è riportato lo schema riassuntivo delle risorse impiegate nei processi operativi.

SCHEMA DI CLASSIFICAZIONE DEGLI ASSET ADOTTATO DALL'ORGANIZZAZIONE

CLASSE	ASSET
Informazioni	- Informazioni relative alle attività operative tipiche dell'organizzazione riguardanti i progetti, i dati dei clienti, i brevetti, le procedure (Critiche - livello A) - Informazioni relative agli aspetti amministrativi dell'attività (Critiche - livello B) - Informazioni relative al sistema di protezione delle informazioni (Critiche - livello A)
Rete e comunicazioni	- Provider (Apparato di fornitura servizi Internet) - Cloud (Server remoto in cui le informazioni vengono duplicate e custodite) - LAN (Rete locale interna all'organizzazione) - Server (Computer che fornisce i servizi di rete interni all'organizzazione) - Router (Dispositivo che permette di interfacciare sottoreti che sono: Primaria, Supporto e Sicurezza) - Switch (Dispositivo di collegamento di altri dispositivi alla rete LAN) - Access point (Dispositivo per l'accesso wireless alla rete) - Client (Computer interni all'organizzazione collegati alla rete) - Cablaggio (cavi Ethernet e fibra ottica)
Software	- Software applicativo - Software sistema informativo - Software di sistema - Software dei dispositivi di elaborazione - Software dei dispositivi di rete - Software degli impianti
Dispositivi per l'elaborazione	- Personal computer portatili - Smartphone - Tablet
Sedi e archivi	- Fabbricato - Area uffici processi primari (Requisiti, progettazione, produzione, etc.) - Area uffici processi di supporto (Amministrazione, organizzazione) - Area uffici sicurezza (Uffici di presidio per la gestione del sistema di sicurezza e i suoi controlli) - Sala server - Archivio cartaceo produzione (documenti afferenti ai processi primari) - Archivio cartaceo amministrativo (documenti afferenti ai processi di supporto) - Database del sistema informativo e database (Primario, supporto e sicurezza)
Impianti e dispositivi di sicurezza	- Proxy (Dispositivo di difesa verso il web che filtra le connessioni in entrata e in uscita) - Cloud (Server remoto in cui le informazioni vengono duplicate e custodite) - Firewall di rete (Dispositivo di monitoraggio del traffico in entrata e in uscita dalla rete LAN) - VPN (Rete privata interna (sicura) creata per la connessione dei computer) - Antivirus (Software di protezione da codice dannoso e malware, programmi cioè che disturbano il funzionamento dei pc) - Software per il log management (software che traccia tutte le operazioni compiute) - Software di gestione dei backup

**FASE DO: COME L'ORGANIZZAZIONE SODDISFA I REQUISITI DELLA FASE****QUALI SONO LE FINALITÀ DEI PROCESSI DI BUSINESS**

Esse, grazie alla rete, entrano nel sistema informativo dell'organizzazione e sono sottoposte alle operazioni dei seguenti processi di cui riportiamo, in sintesi, la finalità:

- **Requisiti** - Raccogliere i dati e le richieste del committente/mercato
- **Progettazione** - Progettare il prodotto/servizio da fornire al committente/mercato, in relazione ai requisiti
- **Outsourcing** - Acquisire dall'esterno quanto necessario per realizzare il prodotto/servizio
- **Produzione** - Realizzare il prodotto/servizio conformemente alla progettazione
- **Preservazione** - Preservare il prodotto realizzato in attesa della consegna
- **Controllo output non conformi** - Gestire e risolvere le non conformità del prodotto/servizio

La logica dell'applicazione dei controlli di sicurezza dell'Annex A ai processi dell'organizzazione costituisce il fondamento del controllo operativo richiesto dalla Norma.

I criteri con cui viene esercitato operativamente il controllo sulla sicurezza delle informazioni sono i seguenti:

IL CONTROLLO OPERATIVO ESERCITATO PER INTEGRAZIONE

La mappatura dei processi identifica le attività di lavoro eseguite e, integrando nel processo il controllo di sicurezza appropriato, l'organizzazione previene i rischi a cui sono sottoposte le informazioni proprio nelle circostanze in cui viene eseguita l'attività di lavoro.

Il controllo di sicurezza, quindi è integrato all'interno della procedura che adotta il personale per eseguire le comuni attività di lavoro. Esso viene eseguito - in genere - proprio in concomitanza della specifica attività di lavoro esposta al rischio.

Le procedure connotate dal prefisso **PROC** (di sistema, ma più in particolare le procedure di business) disciplinano come gestire le attività di lavoro "in sicurezza" per le informazioni trattate al loro interno.

Grazie al criterio dell'integrazione del controllo nel processo, la prevenzione non arriva dall'esterno del processo ma è connaturata con la sua esecuzione. Tale tipo di prevenzione, in genere, è presidiata dal responsabile del processo (RDP) in questione ed è attuata dal personale impiegato nel processo stesso.



FASE DO: PROCESSI E ATTIVITÀ

PROC-810**Pianificazione e controllo operativi****PROC-812 Requisiti**

Raccolta dei requisiti
Determinazione dei requisiti
Riesame dei requisiti
Modifiche ai requisiti

**PROC-813 Progettazione**

Pianificazione della progettazione
Determinazione input progettuali
Riesame della progettazione
Verifica della progettazione
Validazione della progettazione
Determinazione degli output progettuali
Modifiche alla progettazione

**PROC-814 Outsourcing**

Qualifica fornitori abituali
Qualifica nuovi fornitori
Categorie di fornitori e rivalutazioni periodiche
Richiesta di offerta
Analisi dell'offerta e scelta del fornitore
Emissione ordine di acquisto
Modifiche degli ordini
Controlli in ingresso

**PROC-815 Produzione**

Identificazione e rintracciabilità
Validazione della produzione
Rilascio e consegna
Proprietà del cliente
Preservazione
Controllo delle modifiche
Controllo sullo stato di avanzamento
Rilevazione richieste di intervento
Esame della richiesta del cliente
Trattamento e cons. output del post-vendita

In base alla pianificazione e al controllo operativi, l'organizzazione provvede a sottoporre a controllo della verifica sistematica del "valore di rischio accettabile" le seguenti attività.

Le esigenze del cliente/mercato sono codificate in requisiti ben precisi che rappresentano informazioni critiche da proteggere per evidenti motivi connessi agli interessi economici del cliente. I requisiti del cliente permettono all'organizzazione di elaborare progetti il cui interesse economico connesso alla loro "protezione dai rischi" riguarda tanto il cliente che l'organizzazione. I requisiti non si riferiscono alle sole esigenze funzionali del prodotto che il cliente richiede ma anche alle condizioni da applicare per la sicurezza delle informazioni trattate.

I progetti contengono algoritmi con funzioni e calcoli che appartengono al know-how competitivo dell'organizzazione. Possono includere, talora, dati personali, anch'essi da proteggere per la sicurezza degli interessati in base al GDPR.

I requisiti di sicurezza per le informazioni connesse al prodotto da sviluppare sono concepiti già in fase di progettazione per attuare il principio security by design (sicurezza a partire dalla progettazione)

Per realizzare quanto progettato l'organizzazione ricorre anche a fornitori esterni che forniscono processi, prodotti e servizi soltanto a seguito della valutazione della sicurezza con cui gestiscono le informazioni. La nostra organizzazione fa riferimento a fornitori certificati ISO 27001:2024.

Come si nota dalla lettura delle attività di outsourcing, le informazioni trattate sono riservate in quanto riguardano ordini, offerte e di conseguenza trattative commerciali e finanziarie.

Le attività di produzione realizzano di fatto la soluzione che soddisfa i requisiti (funzionali e di sicurezza) raccolti dal cliente.

Esse generano prodotti informatici e tecnologici, software oppure algoritmi o formule che sono "informazioni". La compromissione della loro riservatezza integrità o disponibilità costituirebbe:

- Fonte di danno per l'organizzazione (danni economici e responsabilità 231)
- Fonte di danno per il cliente (responsabilità civile)
- Occasione per ricercare eventuali responsabilità e attivare il procedimento disciplinare

**FASE DO: PROCESSI E ATTIVITÀ****LE PROCEDURE DI SICUREZZA PSI**

Le procedure di sicurezza che, in aggiunta ai processi di business si applicano a tutti i processi, anche quelli di sistema e alle informazioni stesse che esse producono, sono:

PSI-01 Controllo d'accesso

PSI-02 Sicurezza fisica

PSI-03 Lavoro in rete

PSI-04 Preparazione e gestione incidenti

Di queste procedure riportiamo di seguito l'elenco dei controlli di sicurezza (sempre dell'Annex A) che esse disciplinano e la rappresentazione grafica della loro applicazione a tutti i processi del sistema, anche quelli appartenenti alle fasi CHECK e ACT che sono trattate nei paragrafi seguenti del manuale.

ELENCO DEI CONTROLLI APPLICATI ATTRAVERSO LE PROCEDURE DI SICUREZZA PSI**▪ PSI-01 Controllo d'accesso**

- 5.15 Controllo degli accessi
- 5.16 Gestione delle identità
- 5.17 Informazioni di autenticazione
- 5.18 Diritti di accesso
- 8.1 Dispositivi terminali dell'utente
- 8.2 Diritti di accesso privilegiati
- 8.3 Restrizione dell'accesso alle informazioni
- 8.4 Accesso al codice sorgente
- 8.5 Autenticazione sicura

▪ PSI-02 Sicurezza fisica

- 7.1 Perimetri di sicurezza fisica
- 7.2 Accesso fisico
- 7.3 Sicurezza degli uffici, delle stanze e delle strutture
- 7.4 Monitoraggio della sicurezza fisica
- 7.5 Protezione contro minacce fisiche e ambientali
- 7.6 Lavoro in aree sicure
- 7.7 Area di lavoro e schermo puliti
- 7.8 Posizionamento e protezione dell'attrezzatura
- 7.9 Sicurezza dei beni fuori sede
- 7.10 Supporti di memorizzazione
- 7.11 Servizi di supporto
- 7.12 Sicurezza dei cavi

**FASE CHECK: REQUISITI NORMATIVI ATTUATI NELLA FASE**

La nostra organizzazione, in relazione alle scelte di funzionamento del sistema, ha considerato i seguenti requisiti normativi per sviluppare i processi connessi alle attività di verifica della fase CHECK del ciclo di DEMING.

PUNTI NORMA ISO 27001:2024	PARTE CHECK
	REQUISITI NORMATIVI DEL SISTEMA DI GESTIONE
VALUTAZIONE DELLE PRESTAZIONI	9 Valutazione delle prestazioni
	9.1 Monitoraggio, misurazione, analisi e valutazione
	9.2 Audit interno
	9.2.1 Generale
	9.2.2 Programma di audit interno
	9.3 Revisione della direzione
	9.3.1 Generale
	9.3.2 Input per la revisione della direzione
	9.3.3 Risultati della revisione della direzione

I processi della fase CHECK del sistema di gestione si focalizzano sulla valutazione dei risultati di sicurezza generati dal funzionamento del sistema e più in particolare:

- Dai processi di business che integrano i controlli di sicurezza (PROC)
- Dai processi di sicurezza (PSI)
- Dai processi di sistema che, integrando i controlli di sicurezza, forniscono i supporti alle attività operative.

La valutazione inoltre si estende alla conformità e cioè al rispetto dei requisiti normativi da parte del personale e all'idoneità e l'adeguatezza delle risorse sere disponibili.

Le procedure di sistema sviluppate per adempiere ai requisiti normativi appartenenti alla fase CHECK sono le seguenti:

PROC-910 Monitoraggio, misurazione e analisi**PROC-920 Audit interni****PROC-930 Riesame di direzione**

Che rispondono alle necessità di "valutazione delle prestazioni", previste dalla Norma, rispettivamente per:

- I risultati di sicurezza per le informazioni prodotti dai processi e dai controlli di sicurezza applicati (efficacia processi)
- I risultati inerenti alla conformità alla Norma ISO 27001:2024
- I risultati relativi all'efficacia, all'adeguatezza e all'idoneità del sistema in generale

**FASE CHECK: COME L'ORGANIZZAZIONE SODDISFA I REQUISITI DELLA FASE****GLI INDICI DI SICUREZZA PER LE INFORMAZIONI COME INDICATORI DI PERFORMANCE**

L'oggetto del monitoraggio che l'organizzazione esegue mediante la procedura **PROC-910 Monitoraggio, misurazione e analisi** è stato progettato per ottenere una visione ampia della sicurezza delle informazioni vista da molteplici aspetti ad essa connessi, che sono:

- Sicurezza nei ruoli e nei requisiti
- Sicurezza relativa alla tenuta della responsabilità
- Sicurezza relativa alla gestione della rete e delle comunicazioni
- Sicurezza relativa alla gestione del software
- Sicurezza relativa alla gestione dei dispositivi di elaborazione
- Sicurezza relativa alla gestione della sede e degli archivi
- Sicurezza relativa alla gestione degli impianti e dei dispositivi di sicurezza
- Sicurezza relativa alla formazione svolta
- Sicurezza relativa alla gestione della formazione erogata
- Sicurezza relativa alla gestione del piano di formazione
- Sicurezza relativa alla gestione della comunicazione (interna ed esterna)
- Sicurezza relativa alla selezione e alla gestione dei fornitori
- Sicurezza relativa alla gestione dei prodotti non conformi
- Sicurezza relativa alla gestione degli audit e delle non conformità

Il personale esprime il proprio giudizio di valutazione, sistematicamente, in riferimento a tutti questi aspetti e i voti, espressi sotto forma di punteggio che va da 1 a 5 (in senso crescente e migliorativo) permettono di calcolare gli indici di sicurezza. L'organizzazione ha stabilito un indice di sicurezza per ciascuno degli elementi elencati.

Gli indici di sicurezza, che rappresentano il risultato prodotto dai processi del sistema, sono monitorati singolarmente nel tempo e la loro media aritmetica esprime un risultato di sintesi.

La valutazione delle prestazioni dei processi dunque si conclude con l'osservazione di due valori:

- Livello di rischio per le informazioni (stimato dai tecnici)
- Livello di sicurezza effettivamente percepito (stimato dal personale)



FASE CHECK: PROCESSI E ATTIVITÀ

Abbiamo di seguito riportato le attività che si eseguono all'interno dei processi appartenenti alla fase CHECK lasciando che la descrizione permettesse di comprendere la maniera in cui presidiano le performance generali in vista del perseguimento dello scopo.

ATTIVITA' OPERATIVE/PROCESSI

PROC-910 Monitoraggio,
misurazione e analisi

Rilevazione e monitoraggio
Analisi
Valutazione

PROC-920 Audit interni

Pianificazione
Preparazione
Registrazione
Chiusura
Archiviazione
Monitoraggio auditing

PROC-930 Riesame di direzione

Pianificazione e convocazione
Preparazione dei documenti di input
Esecuzione del riesame
Risultanze del riesame
Archiviazione delle informazioni documentate

Durante l'esecuzione delle attività disciplinate dalle procedure l'organizzazione raccoglie le informazioni per calcolare e valutare gli indici di sicurezza delle informazioni riferiti tanto a processi di sistema come ad esempio l'organizzazione del personale quanto a processi di business come la progettazione e la produzione.

I dati sono analizzati statisticamente per produrre delle percentuali che indicano il livello di sicurezza assunto dagli indici. La valutazione avviene in relazione allo scostamento relativo agli obiettivi stabiliti per ciascun indice di sicurezza.

Tale scostamento risulta:

- Fino al 10%, lieve
- Fino al 20%, considerabile
- Fino al 30%, grave
- Fino al 40%, molto grave
- Fino al 50%, gravissimo

Gli audit interni sono pianificati e successivamente condotti da personale qualificato indicato nel **MOD-920-D Registro degli auditor interni**. Grazie all'audit interno l'organizzazione conosce lo stato della propria conformità che incide sull'efficacia di contrasto al rischio per le informazioni.

L'organizzazione per la valutazione di "SCORE" riferita all'applicazione dei controlli dell'Annex A impiega lo strumento CYBERSECURITY SCORE ISO 27001 che rendiconta livelli di sicurezza e lo stato di avanzamento in relazione alla tipologia dei controlli applicati.

Il riesame di direzione considera la struttura e il funzionamento del sistema nel suo complesso. Gli input del riesame sono costituiti dagli output derivanti dagli altri processi e che, riesaminati, permettono all'organizzazione di comprendere se la direzione assunta dall'organizzazione coincide con la direzione in cui è riposto lo scopo da raggiungere.

Attraverso gli output del riesame di direzione invece, l'organizzazione assume precise decisioni intese al miglioramento dell'efficacia, della conformità, dell'adeguatezza e della idoneità che sviluppa e realizza attraverso il processo **PROC-1020 Miglioramento continuo**

**FASE ACT: REQUISITI NORMATIVI ATTUATI NELLA FASE**

La nostra organizzazione, in relazione alle scelte di funzionamento del sistema, ha considerato i seguenti requisiti normativi per sviluppare i processi connessi alle attività di intervento sul sistema della fase ACT del ciclo di DEMING.

PUNTI NORMA ISO 27001:2024	PARTE ACT
	REQUISITI NORMATIVI DEL SISTEMA DI GESTIONE
MIGLIORAMENTO	10 Miglioramento
	10.1 Miglioramento continuo
	10.2 Non conformità e azione correttiva

Questa fase di ACT riceve, come input, gli output generati dalla fase precedente e cioè la fase CHECK. A seguito della valutazione dell'efficacia, della conformità, dell'idoneità e dell'adeguatezza, l'organizzazione interviene attraverso:

- Azioni correttive (intraprese all'occasione) intese a rimuovere eventuali non conformità
- Azioni di miglioramento (intraprese sistematicamente) intese ad aumentare il livello di sicurezza delle informazioni attraverso interventi generali sul sistema che possono consentire di migliorarne l'efficacia. Esse sono presenti nelle strategie di miglioramento che l'organizzazione adotta

LA CHIUSURA DEL CICLO DI DEMING

Attenzione: tali azioni indicate, che ripristinano o migliorano il funzionamento del sistema, sono output dei rispettivi processi disciplinati dalle seguenti procedure:

- **PROC-1010 Non conformità e azioni correttive**
- **PROC-1020 Miglioramento continuo**

Tali output (azioni correttive e di miglioramento) diventano input della fase di PIANIFICAZIONE e, con questo passaggio, assistiamo al compimento del ciclo PLAN, DO, CHECK, ACT che riparte per il ciclo successivo.

Le attività di miglioramento descritte di seguito (eseguite ciclicamente) permetteranno al sistema di gestione delle informazioni, proprio grazie alla loro ciclicità, di:

- Aumentare **continuamente** il livello di sicurezza delle informazioni
- Diminuire **continuamente** il livello di sicurezza delle informazioni

Il sistema, dal punto di vista della sequenza logica dei processi inverte il trattamento dei requisiti normativi 10.1 Miglioramento continuo e 10.2 Non conformità e azione correttiva per una migliore scorrevolezza del flusso. Con la procedura **PROC-1010 Non conformità e azioni correttive** disciplina il trattamento delle singole non conformità rilevate dalle attività di audit, mentre con la procedura **PROC-1020 Miglioramento continuo** dà luogo a azioni di miglioramento intese ad investire la struttura e il funzionamento dell'intero sistema a seguito delle decisioni assunte in fase di riesame di direzione.

**FASE ACT: COME L'ORGANIZZAZIONE SODDISFA I REQUISITI DELLA FASE**

Facendo riferimento alle procedure della fase CHECK, le non conformità emergono nel processo di audit disciplinato dalla procedura **PROC-920 Audit interni**.

L'organizzazione, in base alla procedura **PROC-1010 Non conformità e azioni correttive** provvede dapprima a comprenderle e, soltanto successivamente a trattarle e a verificarne gli esiti di efficacia.

LA GESTIONE DELLE NON CONFORMITÀ

La sequenza delle attività eseguite per la gestione delle non conformità, **PROC-1010 Non conformità e azioni correttive**, è la seguente:

1. Rilevazione della non conformità
2. Classificazione della non conformità
3. Registrazione ed analisi della non conformità
4. Determinazione dell'azione correttiva
5. Attuazione dell'azione correttiva e verifica

I CICLI DI GESTIONE DELLA NON CONFORMITÀ

Il processo di gestione delle non conformità rivolge, nelle prime tre attività, l'attenzione alla non conformità. Le successive due attività, invece, rivolgono l'attenzione all'azione correttiva.

L'organizzazione intende applicare alla gestione delle non conformità due cicli di tipo "while". In logica, un ciclo "while" è un ciclo che si ripete fin quando non è soddisfatta una condizione. Nel nostro caso le condizioni sono due:

1. La comprensione della non conformità:

Fin quando non si comprende la non conformità si ripetono le attività di analisi e non si passa alla attività successiva che riguarda le azioni correttive

2. La verifica di efficacia dell'azione correttiva:

Fin quando non si assicura che l'azione correttiva sia stata efficace, si ritorna sulle attività connesse alla sua rielaborazione e il processo non si chiude

**FASE ACT: COME L'ORGANIZZAZIONE SODDISFA I REQUISITI DELLA FASE****IL MIGLIORAMENTO CONTINUO**

Come la procedura **PROC-920 Audit interni** fornisce gli input alla procedura **PROC-1010 Non conformità e azioni correttive** così, alla stessa maniera e in un disegno logico abbastanza simile, la procedura PROC-930 Riesame di direzione fornisce gli input alla procedura **PROC-1020 Miglioramento continuo**.

La sequenza delle attività eseguite nel processo di miglioramento e disciplinate dalla procedura **PROC-1020 Miglioramento continuo** è molto schematica e rappresenta un vero e proprio processo di ricerca tecnico/scientifica.

L'organizzazione, grazie ai suoi sistemi di raccolta dati e dei relativi database dispone di una considerevole mole di dati che si alimenta ogni giorno. Le informazioni raccolte producono, a loro volta, ulteriori informazioni connesse al loro utilizzo.

L'INFLUENZA DELLA MOLE DI INFORMAZIONI TRATTATA

La crescita esponenziale del volume informazioni trattate dall'organizzazione, per certi aspetti, tende ad aumentare il livello di rischio, in quanto la componente Danno (nel prodotto Probabilità x Danno) si estende ad un crescente numero di informazioni, tale mole di informazioni tuttavia costituisce un patrimonio utile da "analizzare" per migliorare la prevenzione.

LE INDAGINI PREDITTIVE PER LA GESTIONE DEI CAMBIAMENTI

In aggiunta a tutti i dati che le informazioni documentate del sistema consentono di rilevare, l'organizzazione esamina anche i dati (o i meta dati) provenienti dai sistemi. In tale maniera accede ad una visione complessiva del funzionamento del sistema di gestione più ampia che le permette di:

- Interpretare serie storiche di fenomeni connessi alla sicurezza delle informazioni, da cui trarre insegnamento
- Stimare gli andamenti futuri della sicurezza delle informazioni in relazione ai cambiamenti del contesto
- Dare tempestivo seguito all'indagine "predittiva" con azioni mirate ad affrontare i cambiamenti

Le attività eseguite nel processo di miglioramento sono:

1. Raccolta dei dati
2. Analisi dei dati
3. Elaborazione della strategia di miglioramento
4. Implementazione della strategia di miglioramento



FASE ACT: PROCESSI E ATTIVITÀ

Abbiamo di seguito riportato le attività che si eseguono all'interno dei processi appartenenti alla fase ACT lasciando che la descrizione permettesse di comprendere la maniera in cui le azioni correttive e le azioni di miglioramento agiscono in vista del perseguimento dello scopo.

AUDIT

La rilevazione della non conformità oltre a coinvolgere l'auditor rende consapevole anche il responsabile della non conformità nella ricerca delle cause, delle dinamiche, delle conseguenze.

Le non conformità sono classificate in MINORI e MAGGIORI e sono esaminate in relazione alle conseguenze che esse esercitano sul livello di sicurezza delle informazioni.

L'organizzazione elabora le azioni correttive da intraprendere che talora pongono immediatamente fine alla non conformità e alle sue conseguenze mentre invece a volte richiedono dei veri e propri interventi sul sistema di gestione e i suoi asset necessariamente documentati all'interno di una strategia di miglioramento (Es: Azioni di miglioramento anziché Azione correttiva) che mira a scongiurare il ripetersi della non conformità in esame.

All'azione correttiva segue la verifica della sua efficacia che ha un rilevante valore in termini tecnici perché assicura (all'organizzazione), attraverso la dichiarazione documentale della chiusura della non conformità, che il problema è stato risolto.

I dati provenienti dai processi sono raccolti dalle informazioni documentate. Questi dati, unitamente a quelli che provengono dagli altri sistemi, sono analizzati allo scopo di comprendere in che maniera l'organizzazione può assicurare il raggiungimento dello scopo attraverso il miglioramento:

- Dell'efficacia dei processi
- Della conformità alla Norma e all'Annex A
- Dell'idoneità delle sue risorse umane
- Dell'adeguatezza dei supporti resi disponibili ai processi in relazione al livello di rischio da fronteggiare

I risultati delle analisi dei dati permettono all'organizzazione di elaborare ed implementare le necessarie strategie di miglioramento

PROC-1010**Non conformità e azioni correttive**

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

PROC-1020 Miglioramento continuo

Raccolta dei dati
Analisi dei dati
Elaborazione della strategia di miglioramento
Implementazione della strategia di miglioramento

PLAN - NUOVO CICLO