MONITORAGGIO DEL CONTESTO

PROC-400

4 Fattori interni ed esterni che influenzano l'organizzazione

DENOMINAZIONE DEL FATTORE		
Consapevolezza dei rischi da parte dell'alta direzione		
INTERNO/ESTERNO	AMBIENTE E AMBITO	ESTENSIONE GEOGRAFICA
Interno	Persone dell'organizzazione	Locale

DESCRIZIONE DEL FATTORE

Per l'alta direzione è fondamentale essere consapevole dei rischi per la sicurezza delle informazioni in quanto, il funzionamento efficace del sistema di gestione rientra tra le sue responsabilità. Tale consapevolezza deve riguardare anche i rischi provenienti dal comportamento dei propri collaboratori e consulenti. La consapevolezza dei rischi da parte dell'alta direzione incide non poco sui poteri autorizzativi o di delega che l'alta direzione attribuisce al suo staff.

La consapevolezza della direzione si riferisce a quella relativa in materia di impatti ed effetti nel caso di compromissione delle informazioni, incluse le eventuali conseguenze di carattere legale (Dlgs.n.231/2001 etc.).

DENOMINAZIONE DEL FATTORE		
Formazione delle persone nell'ambito della sicurezza delle informazioni e la sicurezza informatica		
INTERNO/ESTERNO	AMBIENTE E AMBITO	ESTENSIONE GEOGRAFICA
Interno	Persone dell'organizzazione	Locale

DESCRIZIONE DEL FATTORE

La formazione tecnica delle persone in materia di sicurezza e cyber sicurezza delle informazioni è un fattore molto influente. Da tale formazione dipende l'impiego efficace dei controlli. Ciò che incide maggiormente sull'applicazione dei controlli per la sicurezza sono i programmi di formazione mirati ad accrescere competenze specifiche del personale in base al ruolo, alle responsabilità ed alle autorità in materia di sicurezza delle informazioni. Non quindi corsi generici o partecipazioni a seminari "globali" ma interventi mirati e selettivi.

DENOMINAZIONE DEL FATTORE		
Evoluzione tecnologica del settore della sicurezza nella gestione delle informazioni		
INTERNO/ESTERNO	AMBIENTE E AMBITO	ESTENSIONE GEOGRAFICA
Esterno	Tecnologico	Internazionale

DESCRIZIONE DEL FATTORE

L'evoluzione tecnologica nell'ambito dell'informatica e della sicurezza delle informazioni (che sono intimamente legate) permette di gestire i controlli per la sicurezza in maniera sempre più efficiente e soprattutto più efficace. Da essa dipende la possibilità di controllare rischi emergenti che l'organizzazione non aveva precedentemente individuato. Il fattore deve essere attentamente monitorato dall'alta direzione e dal responsabile del sistema di gestione delle informazioni che hanno rispettivamente responsabilità di indirizzo e responsabilità di controllo.

5 Esigenze ed aspettative delle parti interessate

A titolo di esempio, le parti interessate e le loro esigenze che influenzano la capacità dell'organizzazione a conseguire i risultati attesi per il proprio sistema di gestione per la sicurezza delle informazioni sono le seguenti:

PARTI INTERESSATE
▪ Clienti
▪ Compagine societaria/proprietaria dell'organizzazione
▪ Investitori
▪ Persone dell'organizzazione

PARTE INTERESSATA
Clienti
Esigenze ed aspettative
L'esigenza dei clienti è quella di poter contare sulla sicurezza dei propri dati che vengono forniti all'organizzazione per poter essere analizzati. L'esigenza di sicurezza riguarda soprattutto la riservatezza in quanto, ove tali dati dovessero accidentalmente o volontariamente essere diffusi e entrare in possesso delle aziende concorrenti, il cliente potrebbe subire dei significativi pregiudizi economici tra i quali la perdita della quota di mercato.
Effetti e potenziali effetti sulla capacità dell'organizzazione
L'esigenza del cliente relativa alla riservatezza dei dati della sua organizzazione incide profondamente sulle scelte degli investimenti in nuove tecnologie da parte dell'organizzazione che, della riservatezza, fa un fattore prestazionale del proprio servizio.

PARTE INTERESSATA
Compagine societaria/proprietaria dell'organizzazione
Esigenze ed aspettative
I soci proprietari dell'organizzazione sono interessati a proteggere dalla divulgazione le informazioni relative ai propri processi di analisi dei dati. Tali informazioni, alla stessa stregua di quelle del committente, se entrassero in possesso di aziende concorrenti, potrebbero minare la business continuity e compromettere il rapporto che l'organizzazione intrattiene con il proprio segmento di mercato. Gli algoritmi e le procedure di analisi dati devono essere protetti anche da eventi che possono comprometterne l'integrità.
Effetti e potenziali effetti sulla capacità dell'organizzazione
L'organizzazione adotta il sistema di gestione per la sicurezza delle informazioni, applicando tutti i controlli previsti dalla Norma ISO 27001:2017 per tutelare il proprio know-how che rappresenta il vero capitale dell'organizzazione.

ORGANIZZAZIONE DEL PERSONALE

3 Modalità operative

L'Alta Direzione ha emanato la Politica per la sicurezza delle informazioni e l'ha diffusa a tutta l'organizzazione attraverso il modulo **MOD-520 - Politica per la sicurezza delle informazioni.**

[controllo 5.1.1] Politica per la sicurezza delle informazioni
Obiettivo: Un insieme di politiche per la sicurezza delle informazioni deve essere definito, approvato dalla direzione, pubblicato e comunicato al personale e alle parti esterne pertinenti.

L'organizzazione del personale è un processo che avviene attraverso le seguenti fasi:

- Determinazione dell'organigramma
- Determinazione dei requisiti e dei ruoli
- Determinazione di mansioni e responsabilità

DETERMINAZIONE DELL'ORGANIGRAMMA

[controllo 6.1] Organizzazione interna
Obiettivo: Stabilire un quadro di riferimento gestionale per intraprendere e controllare l'attuazione e l'esercizio della sicurezza delle informazioni all'interno dell'organizzazione

La direzione garantisce che le responsabilità e le autorità per i ruoli pertinenti siano assegnate, comunicate e comprese all'interno dell'organizzazione mediante la diffusione del **MOD-530-A Organigramma** aziendale per mezzo di:

- Affissione in bacheca
- Pubblicazione sul sito aziendale: www.organizzazione.it/organigramma
- Invio tramite mail alle parti interessate in forma non controllata.

L'alta direzione ha definito le responsabilità e autorità ai fini di:

- Assicurare che il sistema di gestione sia conforme ai requisiti della norma ISO 27001:2017
- Riferire, in particolare all'alta direzione, sulle prestazioni del sistema di gestione per la sicurezza delle informazioni e sulle opportunità di miglioramento

L'alta direzione è l'organo dell'organizzazione che definisce le strategie aziendali. I ruoli, i compiti e le responsabilità relative al Sistema di Gestione per la sicurezza delle informazioni sono individuati dall'alta direzione e riportati nell'organigramma aziendale.

[controllo 6.1.2] Separazione dei compiti
I compiti e le aree di responsabilità in conflitto tra loro sono separati per ridurre le possibilità di uso improprio, modifica non autorizzata o non intenzionale degli asset dell'organizzazione

La direzione individua, per singoli processi, un soggetto con comprovata esperienza il quale, in piena autonomia decisionale e di spesa, organizza sovrintende il processo ad egli affidato assicurando il rispetto dei requisiti del sistema di gestione.

3 Modalità operative

IDENTIFICAZIONE DEI PERICOLI

L'identificazione dei pericoli per la sicurezza delle informazioni viene effettuata attraverso il modulo **MOD-610-A -Identificazione e valutazione del rischio.**

Il primo passo consiste nel raccogliere le seguenti informazioni di base:

- La categoria del processo in cui cercare i rischi
- L'elenco delle informazioni da proteggere
- L'elenco dei documenti che contengono le informazioni da proteggere
- L'elenco dei ruoli dell'organizzazione che sono impegnati nella gestione delle informazioni da proteggere

Il secondo passo consiste nell'individuare, nella categoria di processo considerata, tutti i pericoli presenti. I pericoli, a differenza dei rischi che riguardano sempre e comunque la perdita di riservatezza, dell'integrità e della disponibilità delle informazioni, sono rappresentati dalle cause o dalle circostanze per le quali un determinato evento negativo (pregiudizievole per la sicurezza delle informazioni) può verificarsi.

ANALISI DEI RISCHI

I rischi di perdita della riservatezza, dell'integrità e della disponibilità delle informazioni devono essere analizzati alla luce dei fattori di contesto dell'organizzazione e alla luce delle esigenze e delle aspettative delle parti interessate. Lo scopo dell'analisi è quello di comprendere:

- La maniera in cui i pericoli individuati, nelle dinamiche generali del contesto dell'organizzazione, possano generare eventi pregiudizievoli per le informazioni. Questo sarà utile nella fase di stima della probabilità che tale evento accada.
- Qual è il "valore" delle informazioni che, a seguito del verificarsi dell'eventi pregiudizievole, potrebbero perdere la loro riservatezza, integrità e disponibilità. Questo sarà utile nella fase di stima delle conseguenze (in termini di danno) che tale evento genererebbe.

VALUTAZIONE DEI RISCHI

Per scelta dell'organizzazione i rischi per le informazioni sono sostanzialmente tre:

- Perdita della riservatezza
- Perdita dell'integrità
- Perdita della disponibilità

4 Classificazione delle informazioni e loro etichettatura

[controllo 8.2.1] Classificazione delle informazioni
Le informazioni devono essere classificate in relazione al loro valore, ai requisiti cogenti e alla criticità in caso di divulgazione o modifica non autorizzate

L'organizzazione, alla luce di quanto indicato nei paragrafi precedenti, allo scopo di procedere con un'oculata applicazione dei controlli di sicurezza per le informazioni che tratta, ha classificato queste nella seguente maniera:

Informazioni non critiche
Informazioni trattate dall'organizzazione nell'esecuzione delle proprie attività di business per le quali, la perdita di riservatezza, di integrità e di disponibilità non si ripercuotono in maniera significativa su tutte le parti interessate individuate nell'apposita modulistica di sistema.

Queste informazioni vengono create e scambiate tra i vari attori dei processi dell'organizzazione in maniera conforme a quanto prevedono le fasi dei processi di business in maniera spontanea e non sono sottoposte a controlli di sicurezza

Le informazioni critiche
Le informazioni critiche sono tutte quelle per le quali la perdita di riservatezza, integrità o disponibilità arrecherebbe, alle parti interessate, un pregiudizio significativo di qualunque genere (anche soltanto reputazionale).

Le informazioni critiche sono state divise in due livelli:

- **Informazioni critiche livello A** (quelle trattate nei processi primari e nei processi di sicurezza delle informazioni**)**
- **Informazioni critiche livello B** (quelle trattate nei processi di supporto)

Allo scopo di fugare ogni dubbio in merito alla esatta classificazione di ciascuna informazione, specifichiamo che le indicazioni date sopra servono ad aiutare il personale a riconoscere la classe di appartenenza, dell'informazione in questione, orientandosi in relazione alla categoria del processo:

LIVELLO IC	PROCESSO
A	Primario
A	Sicurezza
B	Supporto

Il criterio, tuttavia, è utile soprattutto quando ci si riferisce ad informazioni scambiate oralmente oppure per iscritto senza impiego dell'apposita modulistica es: si parla di un cliente (informazioni critiche di livello A) al cellulare oppure tramite un testo libero scritto nel corpo della mail.

[controllo 8.2.2] Etichettatura delle informazioni
Deve essere sviluppato e attuato un appropriato insieme di procedure per l'etichettatura delle informazioni in base allo schema di classificazione adottato dall'organizzazione

3 Modalità operative

DETERMINAZIONE DEGLI ASSET IMPIEGATI NEI PROCESSI

L'alta direzione e i ruoli legati alla sicurezza, attraverso l'analisi dei processi, individuano le risorse necessarie (asset) all'attuazione, al funzionamento e al miglioramento del sistema nel **MOD-710-M- Inventario degli asset.**

[controllo 8.1.1] Inventario degli asset
Tutti gli asset associati alle informazioni e alle strutture di elaborazione delle informazioni devono essere identificati; un inventario di questi asset deve essere compilato e mantenuto aggiornato

In tale inventario, che dal punto di vista operativo è compilato e tenuto aggiornato dal RGSI, ciascun asset individuato è stato associato ad una classe ben precisa secondo lo schema riportato di seguito:

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, ecc) ▪ 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)

3 Modalità operative

MONITORAGGIO DELLA SICUREZZA DELL'ASSET

Il monitoraggio avviene nella maniera illustrata in tabella. Per ciascuna classe di "asset" l'RGSI è il responsabile di tutte le fasi di monitoraggio.

CLASSE DELL'ASSET	RESPONSABILE DELLA SICUREZZA DELL'ASSET (CLASSE)	MONITORAGGIO E INDICATORI DI SICUREZZA	RESPONSABILE DEL MONITORAGGIO	PERIODICITÀ
Rete e comunicazioni	AD	Monitoraggio, misurazione e analisi dei risultati ottenuti dai test somministrati al personale che lavora in rete valutato in merito alla sicurezza da: ▪ Minacce fisiche ambientali ▪ Attacchi volontari dall'esterno ▪ Attacchi volontari dall'interno ▪ Eventi per negligenza ▪ Eventi per incompetenza	RGSI	Trimestrale
Software	RDP (PRODUZIONE)	Monitoraggio, misurazione e analisi dei risultati ottenuti dai test somministrati al personale che impiega il software valutato in merito alla sicurezza da: ▪ Minacce fisiche ambientali ▪ Attacchi volontari dall'esterno ▪ Attacchi volontari dall'interno ▪ Eventi per negligenza ▪ Eventi per incompetenza	RGSI	Continuo
Dispositivi per l'elaborazione	AD	Monitoraggio, misurazione e analisi dei risultati ottenuti dai test somministrati al personale che utilizza i dispositivi in merito alla sicurezza da: ▪ Minacce fisiche ambientali ▪ Attacchi volontari dall'esterno ▪ Attacchi volontari dall'interno ▪ Eventi per negligenza ▪ Eventi per incompetenza	RGSI	Trimestrale

3 Controlli per la sicurezza

Le informazioni raccolte dal cliente e trattate successivamente dall'organizzazione sono informazioni critiche di livello A e come tali, conformemente al livello di rischio a cui sono esposte, sono protette dai controlli previsti dall'Annex A (allegato) della norma ISO 27001:2017.

Questo paragrafo dei controlli per la sicurezza, allo scopo di dare un indirizzo chiaro al processo operativo trattato, è presente in ciascuna delle seguenti procedure gestionali *a carattere operativo*:

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

[controllo 12.1] Procedure operative e responsabilità
Assicurare che le attività operative delle strutture di elaborazione delle informazioni siano corrette e sicure

Le attività di lavoro compiute al computer dagli autorizzati sono state individuate, descritte e attribuite secondo quanto documentato nel modulo **MOD-530-C-Matrice delle responsabilità**

[controllo 12.2] Protezione dal malware
Assicurare che le informazioni e le strutture preposte alla loro elaborazione siano protette contro il malware

L'organizzazione ha provveduto all'installazione dell'anti malware grazie al quale provvede alla prevenzione della sicurezza delle informazioni gestite.

Le altre azioni adottate e specificate nella procedura di sicurezza **PSI-12 – Sicurezza operativa** sono le seguenti:

- È installato un adeguato sistema di difesa perimetrale (firewall)
- Sono eseguiti backup periodici assicurandosi che la copia dei dati salvati venga conservata al sicuro
- Vengono aggiornati i sistemi operativi
- Il sistema di rete è dotato di automatizzazione degli aggiornamenti
- Viene verificato che l'anti malware sia sempre aggiornato
- Si proibisce di aprire mail sospette
- Si proibisce di cliccare su aggiornamenti o call to action poco attendibili

5 Premessa generale alle modalità operative

L'organizzazione assicura che i processi, prodotti e servizi forniti dall'esterno siano conformi ai requisiti determinando i controlli da attuare sui processi, prodotti e servizi forniti dall'esterno, quando:

- Prodotti e servizi di fornitori esterni sono destinati ad essere incorporati nei prodotti e servizi dell'organizzazione
- Prodotti e servizi sono forniti direttamente al(ai) cliente(i) da fornitori esterni, per conto dell'organizzazione
- Un processo, o una sua parte, viene fornito da un fornitore esterno, quale esito di una decisione dell'organizzazione.

L'organizzazione ha determinato e applica criteri per la valutazione, selezione, monitoraggio delle prestazioni e per la valutazione periodica dei fornitori esterni, sulla base della loro capacità di fornire processi o prodotti e servizi conformi ai requisiti di sicurezza per le informazioni.

[controllo 15.1.2] Indirizzare la sicurezza all'interno degli accordi con i fornitori
Tutti i requisiti relativi alla sicurezza delle informazioni devono essere stabiliti e concordati con ciascun fornitore che potrebbe avere accesso, elaborare, archiviare, trasmettere o fornire componenti dell'infrastruttura IT per le informazioni dell'organizzazione

L'organizzazione assicura inoltre che i processi, prodotti e servizi forniti dall'esterno non influenzino negativamente la capacità dell'organizzazione di rilasciare con regolarità, ai propri clienti, prodotti e servizi le cui informazioni devono rimanere riservate poiché di livello critico A.

Per il raggiungimento di tale risultato:

- Assicura che le forniture dall'esterno rimangano sotto il controllo del proprio SGSI
- Ha definito i controlli applicabili al fornitore esterno, e agli output risultanti.

L'organizzazione conserva informazioni documentate in merito alla qualifica di "sicurezza" dei fornitori ed in merito ai controlli di sicurezza sul processo di approvvigionamento.

L'organizzazione per la sicurezza relativa alle informazioni ha stabilito i seguenti requisiti per i fornitori:

- Disponibilità per la sicurezza delle informazioni (fornitore motivato)
- Adozione e mantenimento di un SGSI (fornitore che adotta il sistema di gestione)
- Sicurezza delle forniture (servizi/prodotti mai stati contestati in merito a sicurezza)
- Capacità di assistenza per la sicurezza delle informazioni (referenti e uffici indicati)
- Costo /convenienza (costi legati alle misure di sicurezza)

Tali requisiti, in relazione alla fornitura, sono declinati nei contratti di fornitura e sono monitorati affinché si possa avere contezza del loro rispetto da parte del fornitore.

6.1 Valutazione dei fornitori: fasi del processo di qualifica

Il processo di valutazione e qualifica avviene come di seguito descritto:

CATEGORIE DI FORNITORI E RIVALUTAZIONI PERIODICHE

[controllo 15.2.1] Monitoraggio e riesame dei servizi dei fornitori
Le organizzazioni devono regolarmente monitorare, riesaminare e sottoporre a audit l'erogazione dei servizi da parte dei fornitori

I fornitori, a seguito della valutazione, vengono classificati nelle seguenti categorie:

NON QUALIFICATO

Punteggio medio ottenuto da 0 a 2 incluso

Sono fornitori che non sono riusciti a superare il processo di verifica entro il periodo di osservazione. Ad essi viene revocata (o non concessa) la qualifica. Dovranno attendere un periodo prefissato (un anno) di tempo prima di potersi, eventualmente, ripresentare all'Organizzazione per una nuova valutazione.

RDP(ACQUISTI), salvo casi straordinari autorizzati da AD, non può inviare ai fornitori i seguenti:

- **MOD-814-C Richiesta di offerta**
- **MOD-814-D Ordine di acquisto**

QUALIFICATO CON RISERVA

Punteggio medio ottenuto da 2 a 3 incluso

Sono fornitori che sono riusciti a superare il processo di verifica entro il periodo di osservazione, ma con basso punteggio medio. Ad essi viene concessa una qualifica con riserva: possono fornire prodotti/servizi all'Organizzazione, tuttavia gli ordini inviati sono subordinati alla disponibilità (relativamente allo stesso prodotto/servizio) di fornitori qualificati.

RDP(ACQUISTI) può inviare ai fornitori i seguenti:

- **MOD-814-C Richiesta di offerta**
- **MOD-814-D Ordine di acquisto**

Nel corso dell'anno, ad ogni fornitura (o gruppo merceologico omogeneo), RDP(ACQUISTI), eventualmente coadiuvato dai RDP interessati, compila/aggiorna il: **MOD 814-A Elenco fornitori.**

I fornitori qualificati con riserva vengono rivalutati semestralmente a cura di RDP(ACQUISTI).

QUALIFICATO

Punteggio medio ottenuto da 3 a 4 incluso

Sono fornitori che sono riusciti a superare il processo di verifica entro il periodo di osservazione, ritenuti affidabili e competitivi. Ad essi viene concessa una qualifica piena: possono fornire prodotti/servizi all'Organizzazione.
RDP(ACQUISTI) può inviare ai fornitori i seguenti:

- **MOD-814-C Richiesta di offerta**
- **MOD-814-D Ordine di acquisto**

Nel corso dell'anno, RDP(ACQUISTI), eventualmente coadiuvato dai RDP interessati, compila/aggiorna il **MOD-814-A Elenco dei fornitori**

I fornitori qualificati vengono rivalutati annualmente a cura di RDP(ACQUISTI).

MONITORAGGIO, MISURAZIONE E ANALISI

PROC-910

3 Attività operative

MISURAZIONE E MONITORAGGIO

Nella fase di misurazione dei dati da monitorare, l'organizzazione ha provveduto a definire il responsabile ed i relativi supporti documentali:

OGGETTO DEL MONITORAGGIO	RESPONSABILE DELLA RILEVAZIONE E SUPPORTI DOCUMENTALI
Indice di sicurezza nei ruoli e nei requisiti	RGSI rileva l'indice di sicurezza riportato nel modulo MOD-530-B-Ruoli e requisiti e lo riporta nel modulo MOD-910-H-Performance
Indice di sicurezza relativo alla tenuta della responsabilità	RGSI rileva l'indice di sicurezza riportato nel modulo MOD-530-C-Matrice delle responsabilità e lo riporta nel modulo MOD-910-H-Performance
Indice di sicurezza relativo alla gestione della rete e delle comunicazioni	RGSI rileva l'indice di sicurezza espresso nel questionario MOD-710-F- Valutazione rete e comunicazioni e lo riporta nel MOD-710-A-Rete e comunicazioni e nel modulo MOD-910-H-Performance
Indice di sicurezza relativo alla gestione del software	RGSI rileva l'indice di sicurezza espresso nel questionario MOD-710-G- Valutazione software e lo riporta nel MOD-710-B-Software e nel modulo MOD-910-H-Performance
Indice di sicurezza relativo alla gestione dei dispositivi di elaborazione	RGSI rileva l'indice di sicurezza espresso nel questionario MOD-710-H- Valutazione dispositivi per l'elaborazione e lo riporta nel MOD-710-C-Dispositivi per l'elaborazione e nel modulo MOD-910-H-Performance
Indice di sicurezza relativo alla gestione della sede e degli archivi	RGSI rileva l'indice di sicurezza espresso nel questionario MOD-710-I- Valutazione sedi e archivi e lo riporta nel MOD-710-D-Sedi e archivi e nel modulo MOD-910-H-Performance
Indice di sicurezza relativo alla gestione degli impianti e dei dispositivi di sicurezza	RGSI rileva l'indice di sicurezza espresso nel questionario MOD-710-L- Valutazione impianti e dispositivi di sicurezza e lo riporta nel MOD-710-E-Impianti e dispositivi di sicurezza e nel modulo MOD-910-H-Performance
Indice di sicurezza relativo alla formazione svolta	RDP (formazione) rileva l'indice di sicurezza risultante dal modulo MOD-720-D-Test formazione e lo riporta nel modulo MOD-720-C-Registro formazione e nel modulo MOD-910-H-Performance
Indice di sicurezza relativo alla gestione della formazione erogata	RDP (formazione) rileva l'indice di sicurezza risultante dal modulo MOD-720-E-Questionario formazione e RGSI lo riporta nel modulo MOD-720-F-Monitoraggio formazione e nel modulo MOD-910-H-Performance
Indice di sicurezza relativo alla gestione del piano di formazione	RGSI rileva l'indice di sicurezza risultante dal modulo MOD-720-G-Piano formazione annuale e RGSI lo riporta nel modulo MOD-910-H-Performance
Indice di sicurezza relativo alla gestione della comunicazione (interna ed esterna)	RGSI rileva l'indice di sicurezza risultante dal modulo MOD-740-B-Monitoraggio comunicazione e RGSI lo riporta nel modulo MOD-910-H-Performance
Indice di sicurezza relativo alla selezione e alla gestione dei fornitori	RGSI rileva l'indice di sicurezza risultante dal modulo MOD-814-A Elenco fornitori e RGSI lo riporta nel modulo MOD-910-H-Performance
Indice di sicurezza relativo alla gestione dei prodotti non conformi	RGSI rileva l'indice di sicurezza risultante dal modulo MOD-817-B- Prodotti non conformi e RGSI lo riporta nel modulo MOD-910-H-Performance
Indice di sicurezza relativo alla gestione degli audit e delle non conformità	RGSI rileva l'indice di sicurezza risultante dal modulo MOD-920-E-Monitoraggio auditing e RGSI lo riporta nel modulo MOD-910-H-Performance

AUDIT INTERNI

PROC-920

1 Scopo e campo di applicazione

Scopo di questa procedura è definire le modalità operative per la conduzione degli Audit interni attuati dall'organizzazione al fine di verificare la conformità del sistema di gestione per la sicurezza delle informazioni:

- Ai requisiti della norma ISO 27001:2017
- Ai controlli dell'annex A della norma ISO 27001:2017 (come stabiliti dal **MOD-610-B- Piano di sicurezza delle informazioni**)

Altro scopo dell'audit è verificare se il sistema di gestione è efficacemente attuato e mantenuto e se soddisfa tutti i requisiti di sicurezza delle informazioni che l'organizzazione ha stabilito per i propri processi.

[controllo 12.7.1] Controlli per l'audit dei sistemi informativi
I requisiti e le attività di audit che prevedono una verifica dei sistemi di produzione devono essere attentamente pianificati e concordati per minimizzare le interferenze con i processi di business

Il sistema informativo dell'organizzazione è periodicamente "*auditato*". La procedura presente disciplina anche tale audit ma prescrive che l'oggetto dell'audit "sistema informativo" sia specificamente dichiarato all'interno della documentazione in maniera tale da distinguere gli audit specifici sul sistema informativi rispetto agli audit di conformità alle norme.

In tale circostanza, i requisiti ai quali deve risultare conforme il sistema operativo dell'organizzazione sono quelli specificati nelle procedure di sicurezza che seguono, che riportano i singoli controlli di sicurezza indicati dall'Annex A della norma ISO 27001:2017:

- **PSI-12 – Sicurezza operativa**
- **PSI-14 – Acquisizione, sviluppo e manutenzione dei sistemi**

L'organizzazione di tali audit considera la necessità di non influenzare il funzionamento delle attività di business con l'esecuzione delle attività di audit del sistema operativo. Le modalità devono essere specificate nel **MOD-920-B- Piano di audit**.