ELENCO PROCEDURE ISO 27001:2022 – FORMATO MS WORD

www.edirama.org – www.certificazione.info

PROC-07-1 -Procedura per lo sviluppo delle competenze in materia di sicurezza delle informazioni.docx
PROC-07-3 - Procedura_controllo_informazioni_documentate.docx
PROC-09-2 - Procedura Internal-Audit.docx
PROC-09-4 - Procedura riesame della direzione.docx
PROC-10-1 - Procedura gestione non conformita.docx
PROC-A05-10-4 - Procedura gestione Asset.docx
PROC-A05-10-5 - Procedure gestione devices persi o rubati.docx
PROC-A05-12-1 -Procedure classificazione informazioni.docx
PROC-A05-13-1 - Procedura etichettatura informazioni.docx
PROC-A05-14-1 - Procedura trasferimento informazioni.docx
PROC-A05-21-1 - Procedura valutazione del fornitore.docx
PROC-A05-25-1 - Procedura Gestione eventi sicurezza informazioni.docx
PROC-A05-26-1 - Procedura di risposta agli incidenti di sicurezza delle informazioni.docx
PROC-A05-30-3 - Procedura Risposta agli incidenti di continuità ITC.docx
PROC-A05-31-1 -Procedura gestione requisiti legali e contrattuali.docx
PROC-A05-34-2 - Procedura di notifica della violazione dei dati personali.docx
PROC-A06-1-1 - Procedura di screening dei dipendenti.docx
PROC-A06-8-1 - Procedura di segnalazione degli eventi di sicurezza delle informazioni.docx
PROC-A07-10-1 - Procedura di gestione supporti rimovibili.docx
PROC-A07-10-2 - Procedura trasferimento supporti fisici.docx
PROC-A07-14-1 - Smaltimento dei dispositivi.docx
PROC-A07-3-1 - Procedura di accesso al data center.docx
PROC-A07-6-1 - Procedura di lavoro in aree sicure.docx
PROC-A07-9-1 - Procedura di prelievo di asset fuori sede.docx
PROC-A08-8-2 - Procedura Valutazione della vulnerabilità tecnica.docx

ELENCO PROCEDURE ISO 27001:2022 – FORMATO MS WORD

Disponibili su www.edirama.org – www.certificazione.info area ISO 27001

ESEMPIO PROCEDURA RIESAME DELLA DIREZIONE SGSI ISO 27001:2022

Procedura Riesame della direzione SGSI ISO 27001:2022

Indice

1 Introduzione

Lo scopo del presente documento è definire la procedura per l'esecuzione dei riesami della direzione nell'ambito del sistema di gestione gestito da [Nome azienda]in conformità allo standard di sicurezza delle informazioni ISO/IEC 27001.

I riesami della direzione sono una parte fondamentale del sistema di gestione in quanto forniscono un'opportunità regolare per garantire che gli obiettivi vengano raggiunti e che le metriche rientrino in limiti accettabili. Fungono anche da innesco per azioni correttive e da forte stimolo per il miglioramento all'interno dell'SGSI.

2 Riesame della direzione

2.1 Programmazione

il primo giorno lavorativo del trimestre o non appena possibile.

2.2 Partecipanti

Il riesame della direzione sarà presieduto dall'amministratore delegato o da un sostituto nominato. Gli ulteriori partecipanti saranno normalmente i seguenti:

- Direttore operativo (COO)
- Direttore finanziario (CFO)
- Responsabile della privacy
- Responsabile della sicurezza delle informazioni

Le assenze dovrebbero essere comunicate almeno una settimana prima della riunione programmata e, ove possibile, dovrebbe essere nominato un sostituto per partecipare. Ulteriori partecipanti possono essere invitati a discutere specifici punti all'ordine del giorno.

Tutte le riunioni saranno verbalizzate .

2.3 Formato

Per il riesame della direzione verrà utilizzato un modulo standard. Questo modulo verrà aggiornato ogni volta che il contenuto del riesame della direzione deve cambiare, ad esempio per l'aggiunta di ulteriori argomenti di riesame. Nella maggior parte dei casi, il modulo della revisione precedente

può essere utilizzato come punto di partenza, a condizione che vi siano state incorporate eventuali modifiche al contenuto.

I verbali delle riunioni devono essere denominati nel formato "Revisione della direzione [data]" e archiviati come documento Word (. docx) nella cartella [state file location] .

2.4 Classificazione

Il contenuto e il verbale del riesame della direzione saranno trattati come Riservati nell'ambito della definizione dello schema di classificazione delle informazioni in uso all'interno di [Nome azienda]. Ciò significa che occorre prestare la dovuta attenzione per proteggere la riservatezza, l'integrità e la disponibilità dei documenti. Non dovrebbero essere condivisi con terze parti senza che sia stato stipulato un accordo di non divulgazione.

2.5 Preparazione della revisione

Le seguenti azioni devono essere intraprese dal presidente (o dal sostituto nominato) in preparazione del riesame della direzione:

1. Invitare ulteriori punti all'ordine del giorno per la riunione
2. Assicurarsi che le informazioni di supporto richieste per la riunione siano aggiornate dalla persona appropriata, disponibili e distribuite a tutti i partecipanti, tra cui:
    - Rapporti di audit interni ed esterni
    - Rapporti di valutazione del rischio e piani di trattamento
    - Report di monitoraggio e misurazione
    - Registro delle azioni di miglioramento continuo
    - Obiettivi di sicurezza delle informazioni
    - Documentazione SGSI nuova o aggiornata, ad es. politiche
3. Distribuire l'ordine del giorno della riunione e il verbale del riesame della direzione del trimestre precedente
4. Assicurarsi che siano disponibili le risorse necessarie come la sala riunioni, il proiettore e il minute-taker nominato

2.6 Aree esaminate

Le aree coperte dal riesame della direzione possono cambiare nel tempo al mutare dei requisiti aziendali. Alla data della presente procedura sono comprese le seguenti aree:

Rif	Articolo	Descrizione

1	Azioni dalla revisione precedente	Indicare se le azioni sono state completate o meno e, in caso negativo, quali sono i passaggi successivi
2	Modifiche rilevanti per il sistema di gestione	Eventuali cambiamenti interni o esterni significativi verificatisi dall'ultimo riesame che potrebbero avere un impatto sul sistema di gestione e pertanto devono essere presi in considerazione
3	Cambiamenti nei bisogni e nelle aspettative delle parti interessate	Per quelle parti interessate che sono rilevanti per l'SGSI, se le loro opinioni su ciò che l'SGSI deve fornire sono cambiate in qualche modo
4	Non conformità e azioni correttive	Stato delle azioni sollevate da precedenti audit interni ed esterni
5	…… DISPONIBILE NELLA VERSIONE COMPLETA ...	…… DISPONIBILE NELLA VERSIONE COMPLETA ...
6	…… DISPONIBILE NELLA VERSIONE COMPLETA ...	…… DISPONIBILE NELLA VERSIONE COMPLETA ...
7	…… DISPONIBILE NELLA VERSIONE COMPLETA ...	…… DISPONIBILE NELLA VERSIONE COMPLETA ...
8	…… DISPONIBILE NELLA VERSIONE COMPLETA ...	…… DISPONIBILE NELLA VERSIONE COMPLETA ...
9	…… DISPONIBILE NELLA VERSIONE COMPLETA ...	…… DISPONIBILE NELLA VERSIONE COMPLETA ...
10	…… DISPONIBILE NELLA VERSIONE COMPLETA ...	…… DISPONIBILE NELLA VERSIONE COMPLETA ...
11	…… DISPONIBILE NELLA VERSIONE COMPLETA ...	…… DISPONIBILE NELLA VERSIONE COMPLETA ...
12	…… DISPONIBILE NELLA VERSIONE COMPLETA ...	…… DISPONIBILE NELLA VERSIONE COMPLETA ...
13	V	Azioni registrate durante questa revisione, con persona responsabile e data obiettivo
14	…… DISPONIBILE NELLA VERSIONE COMPLETA ...	…… DISPONIBILE NELLA VERSIONE COMPLETA ...

Tabella 1: Aree esaminate

Le azioni registrate verranno tracciate fino al completamento come parte del processo di revisione della direzione.

3 Riesame annuale della direzione

3.1 Programmazione

All'inizio dell'esercizio si terrà un riesame annuale della direzione , in concomitanza con la ripianificazione degli obiettivi di business per l'anno successivo.

3. 2 Partecipanti

Le revisioni annuali della direzione saranno presiedute dall'amministratore delegato o da un sostituto nominato. Gli ulteriori partecipanti saranno normalmente i seguenti:

- Direttore operativo (COO)
- Direttore finanziario (CFO)
- Chief Information Officer (CIO)
- Funzionario capo della privacy (CPO)
- Responsabile della sicurezza delle informazioni
- Responsabili aziendali pertinenti, se del caso

Le scuse dovrebbero essere presentate almeno una settimana prima della riunione programmata e, ove possibile, dovrebbe essere nominato un sostituto per partecipare. Ulteriori partecipanti possono essere invitati a discutere specifici punti all'ordine del giorno.

Tutte le riunioni saranno verbalizzate .

3.3 Formato

Per il riesame annuale della direzione verrà utilizzato un ordine del giorno standard (come definito al punto 3.4 di seguito) che verrà aggiornato ogni volta che il contenuto del riesame della direzione deve cambiare, ad esempio per l'aggiunta di ulteriori argomenti di riesame.

I record devono essere denominati nel formato "Annual Management Review [data]" e archiviati come documento Word (. docx) nella cartella [state file location] .

3.4 Classificazione

Il contenuto dei verbali del riesame annuale della direzione saranno trattati come Riservati nell'ambito della definizione dello schema di classificazione delle informazioni in uso all'interno di [Nome azienda]. Ciò significa che occorre prestare la dovuta attenzione per proteggere la

riservatezza, l'integrità e la disponibilità dei documenti. Non dovrebbero essere condivisi con terze parti senza che sia stato stipulato un accordo di non divulgazione.

3.5 Preparazione della revisione annuale

Le seguenti azioni devono essere intraprese dal presidente (o dal sostituto nominato) in preparazione della revisione annuale della direzione (oltre a quelle per la revisione trimestrale):

- Assicurarsi che le informazioni di supporto richieste per la riunione siano aggiornate dalla persona appropriata, disponibili e distribuite a tutti i partecipanti, tra cui:
    - Dettagli delle modifiche consigliate alla documentazione SGSI
    - Attuale dichiarazione di applicabilità
    - Dettagli dei revisori in carica

3.6 Aree esaminate

In questa revisione, oltre alla consueta agenda trimestrale , saranno esaminate le seguenti aree:

Rif	Attività	Descrizione
1	Revisione della documentazione SGSI	Un rapporto sulla revisione di tutti i documenti all'interno del sistema di gestione per le modifiche ai contenuti, ad esempio aggiornamenti e rimozione di informazioni obsolete, ovvero tutte le politiche, le procedure e gli archivi di informazioni
2	Revisione degli obiettivi	Nuovi obiettivi annuali saranno stabiliti per i prossimi 12 mesi
3	…… DISPONIBILE NELLA VERSIONE COMPLETA ...	…… DISPONIBILE NELLA VERSIONE COMPLETA ...
4	…… DISPONIBILE NELLA VERSIONE COMPLETA ...	…… DISPONIBILE NELLA VERSIONE COMPLETA ...

Tabella 2: aree aggiuntive esaminate durante la revisione annuale

La revisione annuale sarà verbalizzata e le azioni seguite fino al completamento.

	Preparato da:	Recensito da:	Approvato da:	Esempio ELENCO PROCEDURE ISO 27001_2022.docx
Firma				Data entrata in vigore
Data				