TOPCERTIFIER
www.topcertifier.com

# METODOLOGIA DEL SERVIZIO ISO 27001:2013

## INFORMAZIONI GESTIONE DELLA SICUREZZA SSISTEMA (SGSI)

TOPCERTIFIER
www.topcertifier.com

# INTRODUZIONE ALLA NORMA ISO 27001:2013

La norma ISO 27001:2013 consente a un'organizzazione di identificare i rischi per la sicurezza delle informazioni. Prendere in considerazione le minacce, le vulnerabilità, gli impatti e proteggere l'organizzazione senza compromettere la CIA (Confidentiality Integrity Availability) delle informazioni adottandole corretta informazione Sistema di gestione della sicurezza L'obiettivo generale della norma ISO 27001:2013 è quello di coprire gli aspetti seguenti.

- Fornire un modello per stabilire, implementare, operare, monitorare, rivedere, mantenere e migliorare un sistema di gestione della sicurezza delle informazioni con controlli fisici e tecnici.

- Garantire che gli ISMS siano integrati nei processi aziendali delle organizzazioni.

- Creare una cultura organizzativa che incoraggi la partecipazione attiva dei dipendenti al Sistema di gestione della sicurezza delle informazioni.

# CALCIO D'INIZIO

Il kickoff meeting è uno strumento essenziale per comunicare e pianificare l'esecuzione del progetto con un'ostruzione minima e per completare il progetto entro i tempi e i costi pianificati. L'ordine del giorno della riunione iniziale è il seguente:

- Discussione del piano di progetto: include la discussione sulla responsabilità e sulla responsabilità del palo titolari. tappe fondamentali e risultati finali del progetto

- Ambito dei servizi e ambito della certificazione

- Requisiti legali e normativi

# CREAZIONE DEL CORE TEAM

- Nomina del CISO
- Nomina del Comitato per la Gestione della Sicurezza delle Informazioni
- Nomina dei Sindaci
- Responsabile del BCP
- Nomina del Leader ISO

TOPCERTIFIER
www.topcertifier.com

# ANALISI DEL GAP

Durante questa fase conduciamo un'analisi delle lacune per verificare quante delle vostre pratiche attuali sono in vigore in linea con i requisiti standard. le pratiche vengono verificate rispetto a questi quattro criteri di riferimento

- Requisiti della norma ISO 27001:2013
- SOA
- Requisiti legali, statutari e regolamentari
- Requisiti del cliente
- Politiche e procedure interne

I risultati di questa analisi sono presentati sotto forma di Gap Analysis Report. Questo rapporto funziona come elenco di azioni da intraprendere per il promemoria del progetto.

# FORMAZIONE SULLA CONSAPEVOLEZZA DELL'ISMS

ISMS awareness training will be conducted to the employees of your organization. The training session is to help employees to gain knowledge, under stand the concepts of ISO 27001:2013, and align processes and practice towards achieving a secure and threat free work environment. When the staff has been trained they can think & act and contribute towards achieving the goals.

# REGISTRO DEI RISCHI E SOA

Una procedura di gestione del rischio deve essere documentata e utilizzata come riferimento per gestire il rischi identificati in consultazione con tutti i proprietari dei processi e i responsabili funzionali. Utilizziamo la norma ISO 31000 & Tecniche standard di gestione del rischio ISO 27005 per identificare, analizzare, valutare, documentare, dare priorità, trattare e quantificare i rischi identificati. Questo passaggio crea un registro dei rischi. Rischio adatto i piani di trattamento vengono individuati in base al livello di propensione al rischio e al fattore CIA dell'azienda. I risultati di tali azioni vengono calcolati, registrati, valutati e documentati. IL La Dichiarazione di Applicabilità (SOA) definisce e identifica i controlli fisici e tecnici applicabile alla tua organizzazione in base ai processi e ai requisiti aziendali.

TOPCERTIFIER
www.topcertifier.com

# GESTIONE DELLE RISORSE

Assistiamo nello sviluppo di politiche e procedure di gestione patrimoniale coordinandoci con il teste funzionali e comprensione del processo. L'obiettivo principale dell'asset
la gestione è:

- Identificare le risorse organizzative e definire le opportune responsabilità di protezione

- Per impedire la divulgazione, la modifica, la rimozione o la distruzione non autorizzate delle informazioni archiviate sui media

- Garantire che le informazioni ricevano un livello di protezione adeguato in conformità con la sua importanza per l'organizzazione

# SICUREZZA DELLA RETE/COMUNICAZIONE:

Assistiamo nello sviluppo di politiche e procedure di gestione della sicurezza della rete attraverso il coordinamento con i responsabili funzionali e la comprensione del processo. L'obiettivo principale della sicurezza della rete è:

- Garantire la protezione delle informazioni nelle reti e il relativo supporto all'elaborazione delle informazioni strutture

- Per mantenere la sicurezza delle informazioni trasferite all'interno di un'organizzazione e con qualsiasi entità esterna

# GESTIONE DEGLI INCIDENTI

Forniamo assistenza nello sviluppo di politiche e procedure di gestione degli incidenti coordinandoci con il teste funzionali e comprensione del processo. L'obiettivo principale dell'incidente la gestione è:

- Garantire un approccio coerente ed efficace alla gestione della sicurezza delle informazioni incidenti, compresa la comunicazione su eventi e debolezze in materia di sicurezza

TOPCERTIFIER
www.topcertifier.com

# GESTIONE DELLA CONTINUITÀ AZIENDALE

Forniamo assistenza nello sviluppo di politiche e procedure di gestione della continuità aziendale da parte di coordinamento con i responsabili funzionali e comprensione del processo. L'obiettivo principale della gestione della continuità operativa è la seguente:

- Garantire che la continuità della sicurezza delle informazioni sia integrata nell'attività dell'organizzazione sistemi di gestione della continuità

- Garantire la disponibilità di strutture per l'elaborazione delle informazioni

# SICUREZZA FISICA:

Forniamo assistenza nello sviluppo di politiche e procedure di sicurezza fisica coordinandoci con il teste funzionali e comprensione del processo. L'obiettivo principale di Physical la sicurezza è:

- Per prevenire accessi fisici non autorizzati, danni e interferenze all'organizzazione informazioni e strutture di elaborazione delle informazioni

- Per prevenire perdite, danni, furti o compromissioni di beni e interruzioni dell'attività dell' organizzazione operazioni

# SICUREZZA DELLE RISORSE UMANE:

Assistiamo nello sviluppo di politiche e procedure relative alle risorse umane coordinandoci con i responsabili funzionali e comprensione del processo. L'obiettivo principale della sicurezza delle risorse umane è:

- Garantire che i dipendenti e gli appaltatori comprendano le proprie responsabilità e siano idonei a farlo i ruoli per i quali sono considerati

- Per proteggere gli interessi dell'organizzazione come parte del processo di modifica o cessazione occupazione

- Garantire che sia stata impartita una formazione adeguata a tutti i dipendenti e ai fornitori rispetto alla sicurezza delle informazioni

TOPCERTIFIER
www.topcertifier.com

## DOCUMENTAZIONE

I nostri esperti elencheranno le politiche, i processi, le SOP, la SOA applicabile e i record che devono essere implementati definiti e documentati secondo i requisiti ISO 27001:2013 discutendo con ciascuno capi dipartimento e funzione vi assistiamo per la realizzazione della documentazione necessaria.

## STABILIRE I CONTROLLI SGSI

Una volta definite le politiche, i processi, la Dichiarazione di Applicabilità (SOA), i relativi controlli e SOP stato documentato ed è stato elencato l'elenco dei documenti da raccogliere e il personale è stato identificati e formati su tali attività, allora la necessità è di operare, monitorare e rivedere le attività efficienza di tali processi.

## FORMAZIONE PER REVISORI INTERNI

Al personale identificato verrà fornita formazione per auditor interni (IA) ISO 27001:2013. Questa formazione consentirà al personale di analizzare la necessità di IA, pianificare e programmare l'IA e prepararsi liste di controllo di audit, condurre una valutazione d'impatto e documentare e riferire le proprie osservazioni ai vertici gestione.

## AUDIT INTERNO

I nostri esperti supervisioneranno la conduzione dell'audit interno da parte del vostro team di audit interno.  Questo audit interno identificherà le lacune ancora esistenti nel sistema e ne dimostrerà il livello preparazione ad affrontare l'audit di certificazione. Questo audit offre all'organizzazione la possibilità di farlo identificare e rettificare tutte le non conformità prima di procedere all'audit di certificazione. La parte superiorela direzione è informata dei risultati dell'audit interno.

TOPCERTIFIER
www.topcertifier.com

# ANALISI DELLA CAUSA RADICE (RCA) E AZIONI CORRETTIVE

Tutte le non conformità identificate durante l'audit interno, gli audit del cliente o di terze parti o da Metodologia di valutazione e trattamento del rischio, registro dei rischi, registro degli incidenti, vulnerabilità Report VAPT (Assessment & Penetration Test), attacchi malware, registro dei tempi di inattività, rete problemi, controlli di accesso, registro dei beni, rapporti di valutazione dei rischi di terzi, informazioni CIA devono essere elencati la classificazione, gli attacchi interni ed esterni e qualsiasi altra fonte. RCA essere eseguito utilizzando tecniche come il metodo Brainstorming e Fish-Bone. Il correttivo ottimale le azioni vengono implementate. L'efficacia di tali azioni è documentata e verificata tramite a Rapporto sulle Azioni Correttive (CAR).

# RIUNIONE DI REVISIONE DELLA GESTIONE (MRM)

L'MRM è un'opportunità per tutte le parti interessate del SGSI di incontrarsi a intervalli programmati per rivedere, discutere e pianificare azioni sui punti dell'ordine del giorno riportati di seguito.

- Efficacia dell'attuale Sistema di Gestione rispetto al SGSI
- Piani e registrazioni di valutazione e trattamento dei rischi
- Risultati sulla CIA (Confidentiality Integrity & Availability) delle informazioni
- Risultati dell'audit e non conformità provenienti da tutte le fonti
- Piano di azioni correttive per risolvere eventuali questioni aperte
- Miglioramenti continui apportati al sistema
- Risorse e formazione necessarie
- Aspetti normativi e di compliance

# AUDIT DI CERTIFICAZIONE: FASE 1

Quando il livello di preparazione ha raggiunto livelli adeguati, inizia il processo di certificazione inizia. Un auditor nominato dall'Organismo di Certificazione (OdC) verifica lo Standard requisiti tramite un audit di fase 1. Ciò implica che il revisore riveda le politiche, i processi, SOP, SOA, record operativi critici, record IA e MRM. Eventuali deviazioni importanti rispetto ai CB verranno a questo punto comunicate le aspettative per apportare i necessari correttivi. Questo si riduce le possibilità di gravi non conformità durante l'audit di certificazione. Il certificatore TOP fungerà da collegamento con tutte le parti interessate e supervisionare il regolare completamento dell'audit.

TOPCERTIFIER
www.topcertifier.com

# AUDIT DI CERTIFICAZIONE: FASE 2

Una volta completata con successo l'audit di Fase 1, il revisore si concentra su un audit dettagliato del rapporto e documentazione del Sistema di Gestione della Sicurezza delle Informazioni sull'organizzazione. TOPCertifier avrebbe formato il tuo personale sui requisiti di audit e sulla sicurezza affrontare la verifica. I nostri esperti saranno presenti per assistervi con ogni mezzo necessario per il buon svolgimento dell'audit. TOPCertificatore aiuterà il tuo team a risolvere eventuali identificazioni di non conformità durante l'audit. Una volta completato con successo l'audit di certificazione, TOPCertifier collaborerà con tutte le parti Interessato a redigere, approvare e rilasciare il certificato finale.

# CONTINUAZIONE DELLA CONFORMITÀ

TOPCertifier farà parte del percorso di conformità della tua organizzazione e ti assisterà regolarmente intervalli con la formazione necessaria, supporto e aggiornamenti del sistema, audit interni ed esterni e il rinnovo periodico della certificazione.