Information security management systems

FAMIGLIA ISO/IEC 27000

INTRODUZIONE ALLE 27037-27042-27050-1/2/3

DI ANDREA BRACCHI

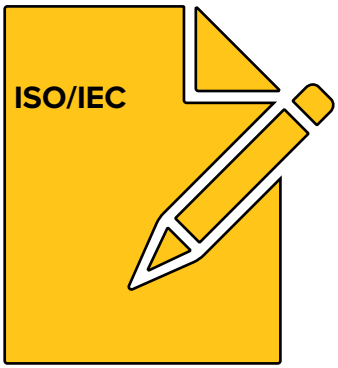
INTRODUZIONE ALLE 27037-27042-27050-1/2/3

DI ANDREA BRACCHI

Verifica il mio profilo personale su Linkedin

StudioBracchi dal 2019
Sede Legale Via della pace n°27
Pontelagoscuro (Ferrara)

visita: **www.studiobracchi.org**
Info**: Studiobracchi.info@gmail.com**


ISO/IEC

PROLOGO

La serie ISO/IEC 27000 è un insieme completo di standard e linee guida che copre tutti gli aspetti della gestione della sicurezza delle informazioni e fornisce un quadro coerente e affidabile per la protezione delle informazioni sensibili e strategiche all'interno di un’organizzazione; questi standard sono riconosciuti a livello globale e sono ampiamente utilizzati.

ISO/IEC 27037

ISO/IEC 27037 è uno standard che fornisce una guida completa per la gestione della sicurezza delle informazioni durante la conduzione di incident response. Questo standard è stato sviluppato per aiutare le organizzazioni a prepararsi e rispondere efficacemente a incidenti di sicurezza informatica.

L'obiettivo principale di ISO/IEC 27037 è quello di aiutare le organizzazioni a garantire che la risposta a un incidente sia efficace, efficiente e coerente con le esigenze di sicurezza delle informazioni dell'organizzazione. Per raggiungere questo obiettivo, lo standard copre diverse aree, tra cui:

1. Preparazione: questa sezione copre la pianificazione e la preparazione per la risposta a un incidente di sicurezza informatica. Incluso anche il coinvolgimento di tutte le parti interessate e la definizione delle responsabilità per la gestione dell'incidente.
2. Conduzione: questa sezione descrive le attività che devono essere effettuate durante la risposta a un incidente, incluso il monitoraggio, la raccolta di informazioni e la valutazione dell'impatto.

3. Ripresa: questa sezione descrive come riprendere le attività normali dopo un incidente e come gestire le attività post-incidente per garantire che l'organizzazione sia pronta a rispondere a futuri incidenti.
4. Comunicazione: questa sezione descrive come comunicare con le parti interessate durante e dopo un incidente, inclusi i clienti, i partner e il pubblico in generale.
5. Miglioramento continuo: questa sezione descrive come valutare e migliorare continuamente le attività di incident response per garantire che l'organizzazione sia sempre pronta a rispondere efficacemente a futuri incidenti.

ISO/IEC 27037 fornisce una guida completa e coerente per la gestione della sicurezza delle informazioni durante la conduzione di incident response, aiutando le organizzazioni a garantire che la loro risposta a un incidente sia efficace, efficiente e coerente con le esigenze di sicurezza delle informazioni dell'organizzazione.

ISO/IEC 27042

La ISO/IEC 27042 è uno standard che fornisce linee guida per la gestione della sicurezza delle informazioni durante la gestione del ciclo di vita delle informazioni. Questo standard copre la gestione della sicurezza delle informazioni durante tutte le fasi del ciclo di vita, inclusa la creazione, la conservazione, la trasmissione, la distruzione e la dismissione delle informazioni.

L'obiettivo principale di ISO/IEC 27042 è quello di aiutare le organizzazioni a garantire che la sicurezza delle informazioni sia integrata in tutte le fasi del ciclo di vita delle informazioni, in modo da proteggere la confidenzialità, l'integrità e la disponibilità delle informazioni.

Questo standard copre diverse aree, tra cui:

1. Pianificazione: questa sezione descrive come pianificare la gestione della sicurezza delle informazioni durante il ciclo di vita delle informazioni.
2. Creazione: questa sezione descrive come garantire la sicurezza delle informazioni durante la creazione di nuove informazioni.
3. Conservazione: questa sezione descrive come proteggere le informazioni durante la conservazione a lungo termine.

4. Trasmissione: questa sezione descrive come garantire la sicurezza delle informazioni durante la trasmissione di informazioni all'interno o all'esterno dell'organizzazione.
5. Distruzione: questa sezione descrive come distruggere in modo sicuro le informazioni non più necessarie.
6. Dismissione: questa sezione descrive come gestire la dismissione di sistemi e dispositivi che contengono informazioni sensibili.

La ISO/IEC 27042 fornisce una guida completa e coerente per la gestione della sicurezza delle informazioni durante il ciclo di vita delle informazioni, aiutando le organizzazioni a garantire che la loro sicurezza delle informazioni sia integrata in tutte le fasi del ciclo di vita delle informazioni.

ISO/IEC 27050-1

La ISO/IEC 27050-1 è uno standard internazionale che fornisce linee guida per la gestione della sicurezza delle informazioni e la gestione dei rischi nella gestione dei dati elettronici. Questo standard si concentra sulla gestione dei rischi e sulla protezione dei dati elettronici durante la loro vita utile, compresa la creazione, la conservazione, la trasmissione e la distruzione dei dati elettronici.

L'obiettivo principale di ISO/IEC 27050-1 è quello di aiutare le organizzazioni a identificare e gestire i rischi associati alla gestione dei dati elettronici, a garantire la protezione dei dati elettronici e a mantenere la loro integrità e disponibilità. Questo standard si concentra sulla gestione dei rischi e sulla protezione dei dati elettronici durante tutte le fasi del loro ciclo di vita.

Questo standard copre diverse aree, tra cui:

1. Pianificazione: questa sezione descrive come pianificare la gestione dei rischi e la protezione dei dati elettronici durante il ciclo di vita dei dati elettronici.
2. Creazione: questa sezione descrive come garantire la protezione dei dati elettronici durante la loro creazione.

3. Conservazione: questa sezione descrive come proteggere i dati elettronici durante la loro conservazione a lungo termine.
4. Trasmissione: questa sezione descrive come garantire la protezione dei dati elettronici durante la loro trasmissione all'interno o all'esterno dell'organizzazione.
5. Distruzione: questa sezione descrive come distruggere in modo sicuro i dati elettronici non più necessari.
6. Sviluppo di procedure: questa sezione descrive come sviluppare e implementare procedure per la gestione dei rischi e la protezione dei dati elettronici.

La ISO/IEC 27050-1 fornisce una guida completa e coerente per la gestione dei rischi e la protezione dei dati elettronici durante il loro ciclo di vita, aiutando le organizzazioni a garantire che i loro dati elettronici siano protetti e gestiti in modo sicuro.

ISO/IEC 27050-2

La ISO/IEC 27050-2 è uno standard che specifica le linee guida per la gestione della sicurezza delle informazioni e la gestione dei rischi nella gestione dei dati elettronici. Questo standard fornisce un insieme di raccomandazioni per la sicurezza delle informazioni e la gestione dei rischi nella gestione dei dati elettronici.

Questo standard copre diverse aree, tra cui:

1. Scelta dei sistemi di gestione dei dati elettronici: questa sezione descrive come scegliere sistemi di gestione dei dati elettronici che soddisfino le esigenze dell'organizzazione in termini di sicurezza delle informazioni e gestione dei rischi.
2. Implementazione dei sistemi di gestione dei dati elettronici: questa sezione descrive come implementare i sistemi di gestione dei dati elettronici in modo sicuro e affidabile.
3. Gestione dei dati elettronici: questa sezione descrive come gestire i dati elettronici in modo sicuro e affidabile durante il loro ciclo di vita.
4. Sicurezza delle informazioni: questa sezione descrive come garantire la sicurezza delle informazioni durante la gestione dei dati elettronici.

5. Gestione dei rischi: questa sezione descrive come gestire i rischi associati alla gestione dei dati elettronici.

La ISO/IEC 27050-2 fornisce una guida completa e coerente per la gestione della sicurezza delle informazioni e la gestione dei rischi nella gestione dei dati elettronici, aiutando le organizzazioni a garantire che i loro dati elettronici siano protetti e gestiti in modo sicuro.

ISO/IEC 27050-3

La ISO/IEC 27050-3 è uno standard internazionale che specifica le linee guida per la gestione della sicurezza delle informazioni e la gestione dei rischi nella gestione delle attività di recupero dati elettronici.Questo standard fornisce raccomandazioni per la gestione della sicurezza delle informazioni e la gestione dei rischi durante le attività di recupero dati elettronici.

Questo standard copre diverse aree, tra cui:

1. Pianificazione del recupero dati elettronici: questa sezione descrive come pianificare le attività di recupero dati elettronici in modo sicuro e affidabile.
2. Implementazione del recupero dati elettronici: questa sezione descrive come implementare le attività di recupero dati elettronici in modo sicuro e affidabile.
3. Recupero dei dati elettronici: questa sezione descrive come recuperare i dati elettronici in modo sicuro e affidabile.
4. Sicurezza delle informazioni: questa sezione descrive come garantire la sicurezza delle informazioni durante le attività di recupero dati elettronici.

5. Gestione dei rischi: questa sezione descrive come gestire i rischi associati alle attività di recupero dati elettronici.

La ISO/IEC 27050-3 fornisce un insieme coerente di linee guida per la gestione della sicurezza delle informazioni e la gestione dei rischi durante le attività di recupero dati elettronici, aiutando le organizzazioni a garantire che i loro dati elettronici siano protetti e gestiti in modo sicuro durante queste attività.

BIOGRAFIA

Da una esperienza di 17 anni in campo, di realizzazione di Procedure a norme ISO, Istruzioni Operative e analisi di Risk management, in ambito di sicurezza sul lavoro nel ruolo di Supervisore, la passione per le nuove discipline che regolano la comunicazione di internet e in ambito web, mi portano ad accostarmi al Diritto informatico.
Lavorando da 4 anni come libero professionista, come consulente privacy, sempre in continuo aggiornamento sia in ambito informatico che in quello giuridico, partecipando a numerosi webinar, workshop, corsi di alta formazione, analisi delle sentenze e certificazioni, approfondisco gli studi iscrivendomi ad un Master in diritto di informatica e certificandomi come DPO.
Gli studi sulla Privacy comparata mi portano ad analizzare più aspetti della materia, quali i reati e crimini informatici, approdando anche alle discipline della Digital Forensics, Cybersecurity, Ingegneria Sociale e Osint.
sono convinto che ogni professione è esercitata da uomini ed è rivolta ad altri uomini.
L'attività lavorativa ha una ricaduta diretta sulla vita dell'uomo e assume quindi, inevitabilmente, un risvolto Etico.