28-30 SETTEMBRE 2022
BARI | VILLA ROMANAZZI CARDUCCI
6° Forum Mediterraneo 2022 in Sanità®

ISO/IEC 27001 in Sanità

La sicurezza come valore aggiunto dei servizi della P.A.

A.O.R.N. S.Giuseppe Moscati – Avellino
Dott. Giuseppe Versace - Direttore U.O.C. Sistemi Informativi

@ForumRisk www.forummediterraneosanita.it

28-30 SETTEMBRE 2022
BARI | VILLA ROMANAZZI CARDUCCI
6° Forum Mediterraneo 2022 in Sanità®

PNRR – Missione 6 Salute (M6.C2 – 1.1.1)

Interventi AORN Moscati:

- Sistema Informativo Sanitario Aziendale Integrato
- Logistica automatizzata del farmaco
- Informatizzazione integrata delle sale operatorie
- Certificazione ISO 27001

28-30 SETTEMBRE 2022
BARI | VILLA ROMANAZZI CARDUCCI
6° Forum Mediterraneo 2022 in Sanità®

Cybercrime business model

- Profilazione del target
  - Superficie di attacco
  - Potenziale economico
- Offerta dei servizi:
  - Fraud as a service
  - Malware as a service
  - Ransomware as a service
  - Attack as a service

28-30 SETTEMBRE 2022
BARI | VILLA ROMANAZZI CARDUCCI
6° Forum Mediterraneo 2022 in Sanità®

Regolamento UE 679/2016 (GDPR), art.42

- c.1: *"gli Stati membri… incoraggiano … meccanismi di certificazione della protezione dei dati … allo scopo di dimostrare la conformità al presente regolamento dei trattamenti effettuati dai titolari del trattamento e dai responsabili del trattamento"*
- c.3: *"La certificazione è volontaria"*
- c.5: *"la certificazione … è rilasciata dagli organismi di certificazione"* accreditati

28-30 SETTEMBRE 2022
BARI | VILLA ROMANAZZI CARDUCCI
6° Forum Mediterraneo 2022 in Sanità®

Lo standard ISO/IEC 27001:2013

- È uno standard di sicurezza informatica redatto dalla ISO (International Organization for Standardization) che ha l'obiettivo fondamentale di proteggere tre aspetti delle informazioni:
  - riservatezza: solo le persone autorizzate hanno il diritto ad accedere alle informazioni
  - integrità: solo le persone autorizzate possono modificare le informazioni
  - disponibilità: le informazioni devono essere accessibili alle persone autorizzate ogni volta che è necessario

28-30 SETTEMBRE 2022
BARI | VILLA ROMANAZZI CARDUCCI
6° Forum Mediterraneo 2022 in Sanità®

Ciclo PDCA (plan-do-check-act)

- specifica dei requisiti e delle linee guida di implementazione e gestione di un "Information Security Management Systems" (ISMS) o "Sistema di Gestione per la Sicurezza delle Informazioni" (SGSI)
- identificazione, analisi, valutazione e trattamento dei rischi
- individuazione degli obiettivi di sicurezza
- definizione del modello aziendale per la valutazione del rischio, la progettazione, l'implementazione e la gestione della sicurezza
- implementazione dei controlli e delle modalità di trattamento dei rischi
- misurazione continua sul funzionamento dei controlli implementati
- miglioramento continuo attraverso audit interni, non conformità, azioni correttive e preventive, sorveglianza

28-30 SETTEMBRE 2022
BARI | VILLA ROMANAZZI CARDUCCI
6° Forum Mediterraneo 2022 in Sanità®

Domini di applicazione

- A.5. Politiche della sicurezza delle informazioni: i controlli in questa sezione descrivono come gestire le politiche della sicurezza delle informazioni
- A.6. Organizzazione della sicurezza delle informazioni: i controlli in questa sezione forniscono lo scenario per l'implementazione della sicurezza delle informazioni definendone l'organizzazione interna (ad es. ruoli, responsabilità, ecc.) e gli aspetti organizzativi di pertinenza (es. gestione dei progetti, uso di dispositivi mobili, telelavoro, etc.)
- A.7. Sicurezza delle risorse umane: i controlli in questa sezione garantiscono che il personale sia formato in materia di sicurezza
- A.8. Gestione delle risorse: i controlli in questa sezione garantiscono che le risorse per la sicurezza delle informazioni (ad es. informazioni, dispositivi di elaborazione, dispositivi di archiviazione, ecc.) siano identificate, che le responsabilità per la loro sicurezza siano designate e che le persone siano istruite al loro corretto utilizzo
- A.9. Controllo degli accessi: i controlli in questa sezione definisco i criteri di accesso alle informazioni e alle risorse informatiche in base alle esigenze aziendali (sia riguardo l'accesso fisico che logico)
- A.10. Crittografia: i controlli in questa sezione forniscono la base per un uso corretto delle soluzioni di crittografia per proteggere la riservatezza, l'autenticità e l'integrità delle informazioni
- A.11. Sicurezza fisica e ambientale: i controlli in questa sezione definiscono le regole per l'accesso autorizzato alle aree fisiche e proteggono le apparecchiature e le strutture da eventi avversi di natura umana o naturale
- A.12. Sicurezza operativa: i controlli in questa sezione garantiscono che i sistemi IT, inclusi i sistemi operativi e i software, siano sicuri e protetti contro la perdita di dati. Inoltre, i controlli in questa sezione richiedono i mezzi per registrare gli eventi e generare evidenze, la verifica periodica delle vulnerabilità e l'audit dei sistemi
- A.13. Sicurezza delle comunicazioni: i controlli in questa sezione proteggono l'infrastruttura e i servizi di rete, nonché le informazioni che viaggiano attraverso di essi
- A.14. Acquisizione, sviluppo e manutenzione del sistema: i controlli in questa sezione assicurano che la sicurezza delle informazioni sia presa in considerazione quando si acquistano nuovi sistemi informatici o si aggiornano quelli esistenti
- A.15. Rapporti con i fornitori: i controlli in questa sezione assicurano che anche le attività esternalizzate svolte da fornitori e partner utilizzino adeguati controlli di sicurezza delle informazioni e descrivono come monitorare le prestazioni relative alla sicurezza di terze parti
- A.16. Gestione degli incidenti della sicurezza delle informazioni: i controlli in questa sezione definiscono lo scenario per la corretta comunicazione, gestione e risoluzione degli eventi avversi in materia di sicurezza
- A.17. Sicurezza delle informazioni nella gestione della continuità operativa: i controlli in questa sezione garantiscono la continuità della gestione della sicurezza delle informazioni e la disponibilità dei sistemi informativi
- A.18. Conformità: i controlli in questa sezione forniscono un quadro per prevenire violazioni e verificare se la sicurezza delle informazioni è implementata ed è efficace in conformità alle politiche, le procedure e i requisiti definiti dalla norma ISO 27001

28-30 SETTEMBRE 2022
BARI | VILLA ROMANAZZI CARDUCCI
6° Forum Mediterraneo 2022 in Sanità®

Conclusioni

- La conformità alla ISO 27001 non solleva l'Azienda dal rispetto della normativa in materia di Privacy e GDPR (il controllo A.18.1.4 richiede, infatti, che *"La protezione dei dati e della privacy deve essere garantita come richiesto nella legislazione"*) ma va oltre l'adempimento di legge in materia di gestione di privacy e di dati personali, interessandosi anche ai dati di business dell'organizzazione ed alla loro salvaguardia.
- I vantaggi principali della certificazione ISO 27001:
  - risparmiare denaro: evitare le sanzioni pecuniarie e le perdite economiche dovute alle violazioni dei dati
  - proteggere la reputazione: dimostrare di aver messo a punto tutte le misure necessarie per proteggere i dati sensibili e di "business"
  - integrare la sicurezza delle informazioni e dei sistemi nella strategia aziendale di gestione del rischio
  - soddisfare le richieste degli stakeholders (legislatore, personale, comunità) dimostrando di affrontare e gestire il rischio
  - ridurre gli incidenti che comportano responsabilità legali e contrattuali

28-30 SETTEMBRE 2022
BARI | VILLA ROMANAZZI CARDUCCI
6° Forum Mediterraneo 2022 in Sanità®

…ma soprattutto

ottenere certificazioni di qualità (quale la ISO 27001) è una libera scelta con cui la P.A. decide di valorizzare e fornire ancora più garanzie alla comunità sulla qualità e l'affidabilità dei servizi che offre

Delitti in materia di violazione del diritto d'autore (Art. 25-novies, D.Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 99/2009]

- Messa a disposizione del pubblico, in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta, o di parte di essa (art. 171, legge n.633/1941 comma 1 lett. a) bis)
- Reati di cui al punto precedente commessi su opere altrui non destinate alla pubblicazione qualora ne risulti offeso l'onore o la reputazione (art. 171, legge n.633/1941 comma 3)
- Abusiva duplicazione, per trarne profitto, di programmi per elaboratore; importazione, distribuzione, vendita o detenzione a scopo commerciale o imprenditoriale o concessione in locazione di programmi contenuti in supporti non contrassegnati dalla SIAE; predisposizione di mezzi per rimuovere o eludere i dispositivi di protezione di programmi per elaboratori (art. 171-bis legge n.633/1941 comma 1)
- Riproduzione, trasferimento su altro supporto, distribuzione, comunicazione, presentazione o dimostrazione in pubblico, del contenuto di una banca dati; estrazione o reimpiego della banca dati; distribuzione, vendita o concessione in locazione di banche di dati (art. 171-bis legge n.633/1941 comma 2)
- Abusiva duplicazione, riproduzione, trasmissione o diffusione in pubblico con qualsiasi procedimento, in tutto o in parte, di opere dell'ingegno destinate al circuito televisivo, cinematografico, della vendita o del noleggio di dischi, nastri o supporti analoghi o ogni altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento; opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico musicali, multimediali, anche se inserite in opere collettive o composite o banche dati; riproduzione, duplicazione, trasmissione o diffusione abusiva, vendita o commercio, cessione a qualsiasi titolo o importazione abusiva di oltre cinquanta copie o esemplari di opere tutelate dal diritto d'autore e da diritti connessi; immissione in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta dal diritto d'autore, o parte di essa (art. 171-ter legge n.633/1941)
- Mancata comunicazione alla SIAE dei dati di identificazione dei supporti non soggetti al contrassegno o falsa dichiarazione (art. 171-septies legge n.633/1941)
- Fraudolenta produzione, vendita, importazione, promozione, installazione, modifica, utilizzo per uso pubblico e privato di apparati o parti di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato effettuate via etere, via satellite, via cavo, in forma sia analogica sia digitale (art. 171-octies legge n.633/1941).

Torna all'inizio