(VIDEOCONFERENZA "MICROSOFT TEAMS")

LA GESTIONE DEI RISCHI ICT

ALLA LUCE DEL

REGOLAMENTO DORA

E DELLE ALTRE NORMATIVE DI SETTORE

Date: **9** e **10 maggio 2024**

Orari: *dalle ore 9.00 alle 13.00 (due mattine)*

Destinatari: Risk Management, Security Management, ICT, Internal Auditing

Introduzione:

La gestione dei rischi ICT è un processo molto articolato, che valuta numerosi parametri e non solo gli aspetti di sicurezza. Una corretta valutazione è indispensabile per determinare quali siano le misure di sicurezza da implementare e gestire, secondo una logica costo/beneficio che deve prendere in considerazione tutte le possibili conseguenze che un evento avverso ha per una organizzazione. Anche per tale motivo non si può parlare di analisi del rischio, ma di analisi dei rischi, in quanto un corretto approccio deve valutare gli impatti dello stesso evento su diverse asset e anche su soggetti terzi rispetto all'organizzazione, che potrebbero rivalersi nei suoi confronti nel caso in cui subissero danni.

[PROGRAMMA]

Ore 8.45 prova collegamento – ore 9.00 apertura dei lavori

I RISCHI

- Il concetto di rischio
- I rischi ICT
- I rischi di soggetti terzi in carico all'organizzazione
- Il rischio di terza e quarta parte

- I limiti dei modelli

LE MINACCE E LE VULNERABILITÀ

LA VALUTAZIONE DEGLI IMPATTI

- Correlazione fra impatti
- Valutazione dell'impatto
- Parametri utili alla valutazione degli impatti

LA VALUTAZIONE DELLA PROBABILITÀ

- Metodologie per la valutazione della probabilità
- Determinazione della probabilità di un evento
- Correlazione fra probabilità
- Le possibili fonti dati per la valutazione della probabilità
- Uso di dati storici e loro profondità

LA GESTIONE DEL RISCHIO

- Standard per la gestione del rischio
- I principi
- I framework
- Il processo per la gestione dei rischi
- Metodologie per la gestione del rischio

L'ANALISI DEI RISCHI

- Terminologia dell'analisi dei rischi
- Metodologie per l'analisi dei rischi
- Fasi dell'analisi dei rischi
- I rischi dell'analisi dei rischi
- Analisi dei rischi dal punto di vista del GDPR: L'analisi del rischio secondo la normativa (artt. 24, 25 e 32) - L' analisi del rischio dal punto di vista dell'organizzazione - Il rischio risarcitorio - Il rischio sanzionatorio
- Il trattamento del rischio dal punto di vista del GDPR e l'esecuzione della DPIA

AGGREGAZIONI E CORRELAZIONI DEI RISCHI

LA BIA (BUSINESS IMPACT ANALYSIS)

- Definizione della metodologia con cui eseguire una BIA
- La conduzione della BIA
- Determinazione del tempo massimo di indisponibilità (MTPD)
- Determinazione dell'RTO
- Individuare gli asset minimi necessari a erogare un processo
- La valutazione delle correlazioni
- La classificazione dei processi
- La valutazione dell'RPO
- Analisi del rischio e BIA

IL TRATTAMENTO DEL RISCHIO

LE MISURE DI SICUREZZA

- Le misure tecniche
- Le misure organizzative

LA GESTIONE DEGLI INCIDENTI

- Rilevazione e gestione
- Classificazione e segnalazioni
- Le violazioni di dati personali

RESILIENZA E CONTINUITA' OPERATIVA

- Gli scenari della continuità operativa
- Le misure per garantire la resilienza
- I piani di continuità operativa

I RISCHI DI TERZE E QUARTE PARTI

- Le attività preliminari
- Il contratto
- Le attività di monitoraggio e di verifiche

GLI ASPETTI NORMATIVI E GLI STANDARD *(Argomenti che saranno trattati congiuntamente agli altri)*

Ore 13.00 chiusura dei lavori

RELATORE: **Giancarlo BUTTI**

Ha acquisito un master in Gestione aziendale e Sviluppo Organizzativo presso il MIP Politecnico di Milano. Membro del Comitato Scientifico del CLUSIT. Si occupa di ICT, organizzazione e normativa dai primi anni 80. Auditor, security manager ed esperto di privacy.

Affianca all'attività professionale a quella di divulgatore con olltre 170 corsi, seminari e master universitari presso ISACA, CLUSIT, ITER, CETIF, IKN, AIIA, UNIVERSITA DI MILANO, POLITECNICO DI MILANO, UNIVERSITÀ DEGLI STUDI SUOR ORSOLA BENINCASA NAPOLI, UNIVERSITA' CA FOSCARI VENEZIA, CEFRIEL, UNISEF,… Ha all'attivo oltre 800 articoli e collaborazioni con oltre 30 testate, 27 fra libri e white paper alcuni dei quali utilizzati come testi universitari; ha inoltre partecipato alla redazione di 29 opere collettive nell'ambito di ABI LAB, Oracle Community for Security, Rapporto CLUSIT… Socio e già proboviro di ISACA/AIEA è socio del CLUSIT, di DFA (Digital Forensis Alumni) e del BCI (Business Continuity Institute), partecipa a numerosi gruppi di lavoro. Ha inoltre acquisito le certificazioni/qualificazioni: LA BS7799, LA ISO/IEC27001, CRISC, CDPSE, ISM, DPO, CBCI, AMBCI.

Quota di partecipazione

comprensiva di materiale didattico su formato elettronico:

Euro 600 + 22% Iva a partecipante

Plus: a tutti i partecipanti verrà fornito (già compreso nella quota di iscrizione) il volume "Manuale di resilienza – Guida pratica alla progettazione gestione e verifica delle soluzioni di resilienza operativa, bunisess continuity e disaster recovery"

Autore: **Giancarlo BUTTI**

N. di pagine: 600

Per iscrizioni e ulteriori informazioni Tel. 02/36577120 - email: informa@informabanca.it