Corso di ***IT Security Governance & Management (Core + Advanced)***

IN-FORMAZIONE SRL - Via Riccardo Grazioli Lante, 9 - 00195 Roma
P.IVA 07252070722 - Tel. : 0687153208 - info@musaformazione.it

CORE LEVEL

MODULO 1

Presentazione del corso, dei suoi obiettivi, e del docente

- Presentazione degli obiettivi del corso
- Presentazione sintetica dei moduli con gli argomenti cronologicamente trattati

Presentazione del docente

Caratteristiche e ruolo di un moderno SI

- schema tipico di un moderno SI, sia on premise, che terziarizzato o un mix dei due (ibrido)
- la necessità di allineare il SI al business
- il piano di evoluzione del business e del SI
- il ruolo dell'architettura ICT per il SI
- la necessità di una effettiva cybersecurity per garantire la continuità operativa (business continuity) di processi/attività chiave per il business
- SI come commodity (almeno per le piccole strutture): è ragionevole? Ha senso?

Gli aspetti organizzativi e normativi per il SI e la sua sicurezza

- il modello demand-delivery
- strutture, ruoli e competenze
- La separazione dei ruoli (SoD, matrici RACI)
- l'interfacciamento ed il controllo dei fornitori ICT-outsourcer
- policy e procedure organizzative
- cenni alle ultime leggi e normative in vigore in Italia
- Esempi di attuazione in strutture organizzative di grandi e di medio-piccole dimensioni.

Approfondimento differenza tra governo (governance) e gestione operativa (management) del SI e della sua sicurezza digitale

- Standard e best practice di riferimento ed il loro posizionamento/confronto nella logica matrice 3x3

Quando, cosa e come terziarizzare della governance e del management operativo

La Governance e la compliance alle principali normative

- La necessità/ opportunità di una approccio "integrato"
- GDPR e normative sulla privacy e la relativa sicurezza
- NIS e NIS 2
- Perimetro di sicurezza nazionale cibernetica (DPCM 30 luglio 2020)
- Cybersecurity Act
- Le normative per la PA (AgID)

Le leggi sul computer crime

Gli Enti italiani ed europei per l'ICT e la sicurezza digitale

- ENISA
- ACN con CSIRT, NCS, CVCN
- Polizia Postale e delle Comunicazioni con CNAIPIC
- COR e altre strutture militari

Altre strutture (NATO, …)

Test Verifica comprensione contenuti Unità 1

MODULO 2

L'allineamento temporale tra il business ed il SI e la sua sicurezza tramite l'architettura ICT

- Cenni sui modelli di business ed i modelli architetturali ICT (standard e best practice)
- Esempi di architetture ICT, partendo dallo standard Togaf
- Esempi di architetture per la sicurezza digitale: NIST, OSA, …
- Le nuove architetture per la sicurezza digitale quali Zero Trust, SASE, SOAR, etc.
- Architetture SI "proprietarie"
    - Microsoft, Oracle, Google, etc.
- Architetture applicative proprietarie
    - SAP, Oracle, Google, AWS, etc.

Terziarizzazioni e cloud

- i pro ed i contro delle terziarizzazioni e dei servizi in cloud
- clausole contrattuali
- SLA e KPI
- Rightsourcing: logiche e criteri per una corretta scelta del/i fornitore/i

La sicurezza digitale

- Che cosa è la sicurezza digitale
- Security by design e by default
- Il processo continuo della sicurezza digitale
    - le sue misure tecniche ed organizzative (prevenzione, contrasto, ripristino, gestione/governo)
- il Framework NIST
- Standard ISO
- Standard NIST ed altri
- Cosa richiede AgID per le PA: CAD e altre normative
- Cosa richiede GDPR
- Il costo della sicurezza digitale ed il costo della "non sicurezza"

la terziarizzazione della sicurezza digitale: MSS e CSaaS

Next Generation Security: le principali innovazioni

che possono impattare sul SI, sulla sua gestione e sulla sua sicurezza digitale

- Strumenti di Intelligenza Artificiale (IA) e di machine Learning (ML)
- Blockchain
- Big Data e Analytics

- Digital twin

Identificazione biometrica utenti e autenticazione passwordless (es. FIDO2)

Cenni alle moderne logiche di sviluppo del software

- Object Orientation e Componentware
- Agile/Extreme/Lean Programming
- DevOps
- Low Code
- Cenni agli ambienti di sviluppo software integrati (IDE, integrated development environment)

Lo sviluppo sicuro di software

Test Verifica comprensione contenuti Unità 2

MODULO 3

La classificazione dei dati ed il loro ciclo di vita (con esempi pratici)

Gli strumenti per la gestione dei dati (Data Catalog, etc.)

Gli attacchi digitali più diffusi e più critici in Italia

- Attacchi target e diffusi
- Dall'indagine OAD di AIPSI
- Da altri rapporti
- L'impatto del Covid-19 e della guerra informatica
- I futuri possibili attacchi più temuti e più probabili

Analisi delle vulnerabilità, dei rischi ICT e dei loro impatti (con esempi e casi pratici)

- Vulnerabilità tecniche, organizzative, delle persone
- il concatenamento delle vulnerabilità dalle infrastrutture alle applicazioni e alla loro gestione
- Come individuare le principali vulnerabilità tecniche
  - CVE/Mitre, US DNS, ed altre fonti
  - OSWAP per le vulnerabilità dei web
  - Cenni agli strumenti di analisi vulnerabilità ICT tipo Nessus, Qualys, OpenVas, etc.
- Dall'analisi delle vulnerabilità ICT all'analisi dei rischi e dei loro impatti
  - Come valutare i possibili impatti di un attacco digitale

Cenni alla simulazione di attacchi e ai pentest

La necessità della continuità operativa (Business Continuity) **e del Piano di Disaster Recovery**

- Standard e best practice di riferimento
- Come impostare un effettivo ed efficace Piano di Disaster Recovery
  - Le varie modalità attuative, ed i criteri di scelta di quale adottare e seguire
- ERT, Emergency Response Team

Simulazione di un DR con DTE, Desk Top Exercise

L'auditing per il SI

- Che cosa è a che cosa serve
- Interno, esterno, mix

- standard di riferimento: Cobit, SAE70, ISAE 3402, SSAE16.

Cenni alle certificazioni

Test Verifica comprensione contenuti Unità 3

ADVANCED LEVEL

MODULO 1

Presentazione del corso, dei suoi obiettivi, e dei docenti

- Presentazione degli obiettivi del corso
- Presentazione sintetica dei moduli con gli argomenti cronologicamente trattati

Presentazione dei docenti

Inquadramento COBIT

- Obiettivi e motivazioni COBIT
- L'evoluzione di COBIT dalle origini (da modello COSO) alla v5 ed alla v. 2019
- I principi ed i fattori abilitanti di Cobit
- Gli stakeholder ed il "valore" per loro

I processi in COBIT

- Processi di governo e di gestione
- I processi dedicati alla sicurezza digitale
- La descrizione in Cobit di un processo
- I livelli di implementazione di un processo

La sicurezza digitale in COBIT

Come, quando e a che condizioni fare riferimento a COBIT

- Cenni alle certificazioni per COBIT
- Esempi di uso, anche parziale di COBIT in strutture organizzative di grandi e di medio-piccole dimensioni.

Cenni ad altri standard e best practice per la governance del SIe della sua sicurezza

- Cenni al Process Capability Model and Levels (ISO/IEC 15504, SPICE)
- Cenni al PAM, Process Assessment Method
- Cenni al CMMI, Capability Maturity Model Integration
- Cenni al BMIS, Business Model for Information Security

Test Verifica comprensione contenuti Unità 1

MODULO 2

Inquadramento ITIL

- Obiettivi e motivazioni
- L'evoluzione di ITIL dalle origini alla v3, la più diffusa in Italia, ed alla rivoluzione della v4 che adotta le logiche di DevOps
- Differenziazione e convergenze/sovrapposizioni con COBIT

I concetti base di ITIL fino alla v.3 (attualmente in funzione nella maggior parte delle organizzazioni che hanno adottato ITIL)

- Fasi, servizi, funzioni, processi, ciclo di un servizio (*service life cycle*), il **valore** (*value*), la **gestione del Servizio** (*Service Management*)
- Il modello ITIL: S**ervice Strategy, Service Design, Service Transition, Service Operation, Continual Service Improvement**. Cenni ai vari processi
    - I processi e le funzioni in SO
- L'importanza della separazione dei compiti e delle responsabilità (SoD, Separation of Duties), le matrici RACI

I nuovi criteri e le nuove logiche della v4

- L'esigenza di far evolvere il modello di Service Management a nuove modalità operative, basata soprattutto alla velocità di intervento, ed esteso dall'UOSI alle altre strutture organizzative e BU (ESM, Enterprise Service Management)
- Lo sviluppo del software ed il suo controllo: Agile, Lean DevOps
- Eliminazione delle fasi, passaggio dai processi alle practices (ma mantenendo molto dei concetti e delle logiche delle prime)
- Leadership IT e Organizational Change management
- L'integrazione del concetto di Service Integration and Management in contesti Multivendor
- La Governance del SI e della sua sicurezza in ITIL

La sicurezza digitale in ITIL

Come, quando e a che condizioni fare riferimento a ITIL

- Cenni alle certificazioni per ITIL
- Esempi di uso, anche parziale di ITIL in strutture organizzative di grandi e di medio-piccole dimensioni
- Un approccio ibrido con COBIT e ITIL?

Test Verifica comprensione contenuti Unità 2

MODULO 3

Come gestire la governance ed il management di un SI e della sua sicurezza digitale

- L'impossibilità/non convenienza ad automatizzare la Governance del SI
- La necessità di automatizzare quanto più possibile la gestione operativa
- Logiche e criteri di cosa e come terziarizzare o non
- Governare il SI
    - I rapporti con gli utenti
    - I rapporti con gli stakeholders
    - Piano strategico pluriennale di business allineato al piano evolutivo SI
    - La trasformazione digitale
- Gestione operativa del SI
    - Monitoraggio e controllo funzionalità e prestazioni intero SI
    - Monitoraggio e controllo sicurezza digitale
    - Gestione problemi (Help Desk e trouble ticketing**)**
    - Gestione incidenti e disastri
    - Gestione accessi utenti privilegiati e finali
    - Provisioning
    - Gestione backup ed eventuali ripristini
    - Piano di Disaster Recovery e sua attuazione
    - Capacity planning
- Il Supporto informatico alle decisioni: uso di tecniche di Intelligenza Artificiale e di Machine Learning

Cenni agli strumenti usabili e casi reali di implementazione/attuazione

- Gli strumenti: cenni alle soluzioni proprietarie disponibili sul mercato ed a quelle open
- Esempi di attuazione in strutture organizzative di grandi e di medio-piccole dimensioni (su diretta esperienza del docente)

Analisi del valore del SI

- Che cosa è a che cosa serve
- Esempio di strumento per effettuarla in maniera semplificata con casi reali anche nelle PMI
- Esempi di calcolo di del valore dell'ICT "as is" e "to be" con lo strumento di Malabo

I possibili finanziamenti per il SI e la sua sicurezza digitale

- La leva della trasformazione digitale
- I finanziamenti nazionali e a livello regionale/provinciale
- I finanziamenti dai progetti europei

I finanziamenti con il PNRR

Test Verifica comprensione contenuti Unità 3