ALLEGATO "3"

[K1.8] ESPERTO IN SICUREZZA INFORMATICA

Descrizione sintetica:
L'Esperto in sicurezza informatica opera in autonomia, con diretta responsabilità, al fine di garantire la protezione dei sistemi rispetto alle possibili minacce e criticità di funzionamento. Come tale, testa: la sicurezza dei sistemi contro intrusioni, virus e minacce - intenzionali o ambientali - la recuperabilità di dati e operazioni a seguito di incidenti o malfunzionamenti e la corretta funzione di criptaggio e cifratura; testa e corregge bug e falle, sviluppando adeguate misure preventive; progetta e supervisiona la formazione agli utenti dei sistemi, in merito alle buone pratiche per la sicurezza informatica.

SISTEMI DI REFERENZIAZIONE	
Sistema di riferimento	**Denominazione**
Settore economico-professionale (S.E.P.)	Servizi di informatica
Area/e di Attività (AdA) del Repertorio nazionale delle qualificazioni regionali a cui il profilo afferisce	[14.01.07] Implementazione di misure di sicurezza dei sistemi informativi
Livello E.q.f.	6
Posizione classificatoria ISTAT CP 2011	2.1.1.5.4 - Specialisti in sicurezza informatica
Posizione/i classificatoria/e ISTAT ATECO 2007	62.02.00 - Consulenza nel settore delle tecnologie dell'informatica 62.09.09 - Altre attività dei servizi connessi alle tecnologie dell'informatica nca 62.01.00 - Produzione di software non connesso all'edizione 63.11.20 - Gestione database (attività delle banche dati)

UNITÀ DI COMPETENZA – Analisi delle vulnerabilità software e hardware e della conformità alla normativa vigente
RISULTATO ATTESO DALL'ESERCIZIO DELLA COMPETENZA Analizzare sistemi informativi, per le componenti hardware e software, dati ed operazioni, al fine di rilevarne rischi di sicurezza e vulnerabilità rispetto alle possibili minacce ed alla continuità di funzionamento ed integrità, individuando ed applicando metodi e norme di riferimento e supportando i relativi processi decisionali di adeguamento
LIVELLO E.q.f.: 6
CONOSCENZE • Architettura hardware e software dei sistemi digitali • Metodi di analisi dei rischi di sicurezza e di individuazione delle vulnerabilità per la sicurezza di sistemi informatici

- Metodi di analisi dei punti di forza e di debolezza in relazione alle esigenze di sicurezza e protezione dei dati
- Fondamenti teorici della sicurezza dei sistemi informativi
- Metodi di valutazione dei rischi per la sicurezza legati alle componenti hardware e software del sistema
- Metodi di valutazione di rischi per la sicurezza legati alle componenti del sistema informativo dedicate al networking (protocolli, connessioni, apparecchiature di rete)
- Tipologia delle potenziali minacce all'integrità, riservatezza e disponibilità delle informazioni e delle risorse di un sistema informativo o di una rete
- Normativa in materia di sicurezza informatica e relativa certificazione
- Normativa in materia di protezione dei dati trattati con sistemi informatici
- Inglese tecnico per l'informatica

ABILITA'

- Allestire e manutenere asset inventory
- Analizzare l'architettura del sistema informativo per individuare i possibili punti di attacco al sistema o alle informazioni in esso contenute
- Analizzare i requisiti richiesti al sistema informativo dalle previsioni normative vigenti in materia di privacy e sicurezza informatica
- Individuare le vulnerabilità dell'architettura, delle apparecchiature hardware, del software e dei processi di gestione del sistema informativo
- Elaborare documenti di valutazione dei rischi per la sicurezza del sistema informativo, contenenti l'analisi delle minacce e delle vulnerabilità individuate e delle possibili contromisure
- Interagire con i responsabili dei vari livelli decisionali, orientando e supportando le scelte strategiche in materia di sicurezza dei sistemi informativi

INDICATORI DI VALUTAZIONE DEL POSSESSO DELLA COMPETENZA

Sulla base di indicazioni relative a tipologie di sistemi informativi ed all'insieme delle tipologie di potenziali minacce, analizzare i livelli di sicurezza di sistema – per le componenti hardware e software –, dati ed operazioni, individuando lo stato di conformità, con riferimento alle norme applicabili e gli elementi problematici

PRESTAZIONE MINIMA ATTESA IN ESITO ALLA VALUTAZIONE

Per almeno una tipologia di sistema informatico e con riferimento all'insieme delle potenziali minacce, sulla base delle indicazioni date, individuazione delle norme applicabili ed analisi dei livelli di sicurezza, conclusa da redazione di report indicante l'approccio seguito e le problematiche di vulnerabilità/non conformità rilevate

MODALITÀ DI VALUTAZIONE DEL POSSESSO DELLA COMPETENZA

Audizione, colloquio tecnico e/o prova prestazionale

UNITÀ DI COMPETENZA – Definizione e implementazione di soluzioni per la sicurezza dei sistemi hardware e software

RISULTATO ATTESO DALL'ESERCIZIO DELLA COMPETENZA

Definire ed implementare, sulla base dell'esito di analisi di vulnerabilità, soluzioni tecniche di protezione del sistema informatico, agendo sulle diverse componenti e funzioni, mediante tecniche di configurazione e specifici applicativi

LIVELLO E.q.f.: 6

CONOSCENZE

- Tipologie e logiche di funzionamento dei programmi informatici creati per la violazione o il danneggiamento dei sistemi informativi (virus, worm, Trojan, malware, ecc…)
- Tipologie e caratteristiche degli attacchi al sistema informativo a livello di IP, TCP/UDP, protocollo applicativo, applicazione, utente
- Caratteristiche e funzionalità dei firewall
- Metodi e tecniche di configurazione del sistema di protezione e del firewall
- Modalità di autorizzazione e controllo del traffico fra reti e tipologie di tentativi di violazione delle politiche di sicurezza
- Caratteristiche e funzionalità dei programmi di network scanning ed intrusion detection
- Caratteristiche e funzionalità dei proxy e del controllo di connessioni e traffico TCP/IP da client a server
- Sistemi di autorizzazione degli accessi al sistema informativo ed alle reti
- Normativa in materia di sicurezza informatica e relativa certificazione
- Normativa in materia di protezione dei dati trattati con sistemi informatici
- Inglese tecnico per l'informatica

ABILITA'

- Utilizzare programmi di crittografia e cifratura per la protezione dei dati contenuti nel sistema informativo e delle comunicazioni con l'esterno
- Rafforzare l'architettura della rete con la creazione di Zone Demilitarizzate (DMZ), per la protezione della rete informatica e del sistema informativo, dai tentativi di attacco e violazione provenienti dall'esterno
- Installare e configurare proxy e firewall, per garantire la sicurezza, la riservatezza e l'integrità delle connessioni tra client e server
- Installare e configurare un efficace ed efficiente software antivirus o EDR, per l'individuazione e la rimozione dei programmi informatici finalizzati alla violazione o al danneggiamento del sistema informativo
- Installare e configurare sistemi di autenticazione, autorizzazione e controllo degli accessi (IAM), che garantiscano la sicurezza del sistema informativo senza creare difficoltà agli utenti autorizzati
- Definire profili di accesso selettivi, individuali o per gruppi omogenei (configurazione dello IAM), basati su effettive necessità operative o su autorizzazioni preventivamente approvate
- Definire le credenziali di autenticazione per l'identificazione degli utenti autorizzati ad accedere al sistema informativo, prevedendo l'utilizzo delle tecniche più appropriate (user-id, password, smart card, sistemi biometrici, etc.)
- Progettare un Security Operation Center (SOC)

INDICATORI DI VALUTAZIONE DEL POSSESSO DELLA COMPETENZA

Sulla base di indicazioni relative a tipologie di sistemi informativi, esiti dell'analisi della loro vulnerabilità ed all'insieme delle tipologie di potenziali minacce, definire le operazioni tecniche da compiere, per garantire il livello di protezione definito ed indicare o svolgere le relative modalità di implementazione

PRESTAZIONE MINIMA ATTESA IN ESITO ALLA VALUTAZIONE

Per almeno una tipologia di sistema informatico e con riferimento all'insieme delle potenziali minacce, sulla base delle indicazioni sulla vulnerabilità date, motivata individuazione delle

operazioni tecniche di protezione e delle relative modalità di implementazione, anche in situazione simulata

MODALITÀ DI VALUTAZIONE DEL POSSESSO DELLA COMPETENZA
Audizione, colloquio tecnico e/o prova prestazionale

UNITÀ DI COMPETENZA – Monitoraggio e ripristino della sicurezza di sistemi hardware e software

RISULTATO ATTESO DALL'ESERCIZIO DELLA COMPETENZA
Monitorare lo stato di sicurezza dei sistemi informatici, verificando l'efficacia delle soluzione di protezione adottate ed intervenendo in caso di attacchi o problemi, ripristinando le condizioni operative di sicurezza ed integrità

LIVELLO E.q.f.: 6

CONOSCENZE

- Principali tecniche di attacco alla sicurezza informatica
- Tipologie e logiche di funzionamento dei programmi informatici creati per la violazione o il danneggiamento dei sistemi informativi (virus, worm, Trojan, malware, ecc…)
- Caratteristiche e funzionalità dei firewall
- Tecniche e sistemi di crittografia e cifratura
- Tecniche e strumenti di rilevazione e prevenzione intrusioni
- Sistemi di autorizzazione degli accessi al sistema informativo ed alle reti
- Identity management system (IMS)
- Principi di organizzazione e gestione della sicurezza informatica
- Documenti di business continuity
- Tecniche di disaster recovery
- Normativa in materia di sicurezza informatica e relativa certificazione
- Normativa in materia di protezione dei dati trattati con sistemi informatici
- Inglese tecnico per l'informatica

ABILITA'

- Utilizzare sistemi di Security Information Event Management (SIEM)
- Ripristinare integrità, funzionamento e livello di sicurezza, in seguito ad una violazione tentata o riuscita della sicurezza del sistema informativo
- Controllare il rispetto delle misure di sicurezza progettate
- Testare il funzionamento dei piani di business continuity e disaster recovery
- Utilizzare identity management system (IMS)
- Riconoscere e bloccare attacchi denial of service
- Monitorare e bloccare il traffico interno ed esterno, che costituisca una potenziale minaccia alla sicurezza del sistema informativo
- Adottare le opportune contromisure in caso di attacco alla sicurezza del sistema informativo (hardware e software)
- Monitorare ed interpretare log (server, dispositivi di rete, applicazioni, ecc.)
- Utilizzare tecniche e sistemi di crittografia e cifratura
- Individuare ed eliminare malware (spyware, backdoor, trojans, ecc.)
- Gestire le regole di firewall

INDICATORI DI VALUTAZIONE DEL POSSESSO DELLA COMPETENZA

Sulla base di indicazioni relative a tipologie di sistemi informativi, impostare il processo di monitoraggio e, dato un insieme di casi di minaccia/criticità, individuare e porre in atto le contromisure e le operazioni necessarie, per ripristinare le condizioni operative di sicurezza ed integrità

PRESTAZIONE MINIMA ATTESA IN ESITO ALLA VALUTAZIONE

Per almeno una tipologia di sistema informatico e con riferimento a casi di minaccia/criticità dati, motivata impostazione del processo di monitoraggio ed applicazione, in situazione simulata, delle coerenti contromisure ed operazioni necessarie, per ripristinare le condizioni operative di sicurezza ed integrità

MODALITÀ DI VALUTAZIONE DEL POSSESSO DELLA COMPETENZA

Audizione, colloquio tecnico e/o prova prestazionale

UNITÀ DI COMPETENZA – Definizione ed adozione delle misure organizzative per la sicurezza del sistema informativo

RISULTATO ATTESO DALL'ESERCIZIO DELLA COMPETENZA

Definire, sulla base del rapporto fra costi e benefici, l'insieme delle misure organizzative e dei comportamenti necessari, per garantire la sicurezza dei sistemi informativi, individuando ruoli, responsabilità, procedure e modalità di audit e curando la formazione delle risorse umane a vario titolo interessate

LIVELLO E.q.f.: 6

CONOSCENZE

- Principali tecniche di attacco alla sicurezza informatica
- Strumenti e tecnologie per la protezione fisica delle strutture, per assicurare la sicurezza dei locali e delle componenti del sistema informativo, dai rischi ambientali connessi: ad interruzioni dell'alimentazione, incidenti, danneggiamenti, calamità naturali
- Metodologie per l'organizzazione di un sistema di internal auditing, per verificare l'effettivo livello di sicurezza dei sistemi informativi
- Tecniche di backup e di restore dei sistemi informativi
- Tecniche di analisi dei costi e dei benefici, dell'adozione di modelli organizzativi finalizzati all'incremento del livello di sicurezza dei sistemi informativi
- Tecniche di progettazione dell'organizzazione per la sicurezza: divisione delle responsabilità e definizione delle funzioni
- Tecniche di formazione degli utenti finali e delle professionalità interessate dal mantenimento della sicurezza del sistema informativo
- Normativa in materia di sicurezza informatica e relativa certificazione
- Normativa in materia di protezione dei dati trattati con sistemi informatici
- Inglese tecnico per l'informatica

ABILITA'

- Programmare un piano di audit e controlli sulla sicurezza, per verificare l'effettivo livello di protezione del sistema informativo
- Organizzare una gestione efficace delle emergenze, con una chiara definizione dei ruoli e delle procedure ed una corretta attribuzione delle responsabilità, in caso di incidente o attacco informatico
- Organizzare le procedure per il controllo dei log, degli accessi e del traffico verso l'esterno,

del sistema informativo

- Elaborare i piani di Disaster Recovery e Business Continuity che, in caso di incidente grave o interruzione per cause non controllabili, consentano il mantenimento o il ripristino, nel più breve tempo possibile, della corretta funzionalità del sistema informativo
- Definire gli strumenti, l'organizzazione, i ruoli e le responsabilità, per garantire una corretta gestione della sicurezza del sistema informativo
- Orientare e supportare il processo di adeguamento delle competenze e dei comportamenti di sicurezza informatica, di tutti i membri dell'organizzazione

INDICATORI DI VALUTAZIONE DEL POSSESSO DELLA COMPETENZA

Sulla base di indicazioni relative a tipologie di sistemi informativi e caratteristiche organizzative, impostare la definizione di strumenti, ruoli e responsabilità, per garantire una corretta gestione della sicurezza del sistema, valutando ipotesi alternative, sulla base di criteri di costo/beneficio

PRESTAZIONE MINIMA ATTESA IN ESITO ALLA VALUTAZIONE

Per almeno una tipologia di sistema informatico e con riferimento ad un set di caratteristiche organizzative date, motivata impostazione di almeno due alternative di strumenti, ruoli e responsabilità, valutate comparativamente in termini di costi e benefici

MODALITÀ DI VALUTAZIONE DEL POSSESSO DELLA COMPETENZA

Audizione, colloquio tecnico e/o prova prestazionale