Responsabile Sicurezza Sistemi Informativi (Security Manager)

Mi Formo e lavoro

DURATA

210 ore

DESTINATARI

I destinatari delle azioni finanziate a valere sul presente Avviso devono essere in possesso dei seguenti requisiti:

- essere residenti o domiciliati in un Comune della Regione Puglia. Se cittadini non comunitari devono essere in possesso di regolare permesso di soggiorno che consente attività lavorativa;
- avere compiuto il 18esimo anno di età;
- essere disoccupati secondo la definizione di cui all'art. 19 del D.lgs 150/2015 e privi di strumenti di sostegno al reddito;
- essere disoccupati secondo quanto definito dall'art. 19 del D.lgs 150/2015 e beneficiari di strumenti di sostegno al reddito.

CONTENUTI

Denominazione AdA	progettazione ed implementazione delle misure tecniche per la sicurezza del sistema informativo
Descrizione della performance	progettare ed implementare tutte le misure tecniche, relative sia alle componenti hardware che software, necessarie per assicurare al sistema informativo un livello di sicurezza informatica che consenta di ridurre il rischio entro limiti ritenuti accettabili
Unità di competenza correlata	1141
Capacità	installare e configurare sistemi di autenticazione, autorizzazione e controllo degli accessi che garantiscano la sicurezza del sistema informativo senza creare difficoltà agli utenti autorizzati 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, ecc...) definire profili di accesso selettivi, individuali o per gruppi omogenei, basati su effettive necessità operative o su autorizzazioni preventivamente approvate installare e configurare un efficace ed efficiente software antivirus per l'individuazione e la rimozione dei programmi informatici finalizzati alla violazione o al danneggiamento del sistema informativo installare e configurare un proxy, per garantire la sicurezza, la riservatezza e l'integrità delle connessioni tra client e server 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 utilizzare programmi di crittografia e cifratura per la protezione dei dati contenuti nel sistema informativo e delle comunicazioni con l'esterno
Conoscenze	caratteristiche e funzionalità dei firewall, per controllare il traffico fra due o più reti, permettendo solo quello autorizzato e rilevando e segnalando

	eventuali tentativi di violazione delle politiche di sicurezza definite caratteristiche e funzionalità dei programmi informatici di network scanning ed intrusion detection, per individuare e neutralizzare i tentativi di accesso non autorizzato al sistema informativo caratteristiche e funzionalità dei proxy, per controllare le connessioni e il traffico tcp/ip da client a server in modo da impedire intrusioni e violazioni del sistema informativo tipologie e caratteristiche degli attacchi al sistema informativo a livello di ip, tcp/udp, protocollo applicativo, applicazione, utente, per operare una corretta configurazione del sistema di protezione e del firewall, in modo da prevenire e controllare le violazioni del sistema informativo tipologie e logiche di funzionamento dei programmi informatici creati per la violazione o il danneggiamento dei sistemi informativi (virus, worm, trojan, malware, ecc...) sistemi di autorizzazione degli accessi al sistema informativo, per assicurare l'accesso degli utenti autenticati soltanto ad aree predefinite del sistema
Denominazione AdA	definizione ed adozione delle misure organizzative per la sicurezza del sistema informativo
Descrizione della performance	definire ed adottare tutte le misure organizzative, relative sia al personale che alle infrastrutture, necessarie per garantire al sistema informativo un livello di sicurezza che consenta di ridurre il rischio entro limiti ritenuti accettabili
Unità di competenza correlata	1142
Capacità	organizzare le procedure per il controllo dei log, degli accessi e del traffico verso l'esterno del sistema informativo definire gli strumenti, l'organizzazione, i ruoli e le responsabilità per garantire una corretta gestione della sicurezza 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 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 programmare un piano di audit e controlli sulla sicurezza, per verificare l'effettivo livello di protezione del sistema informativo
Conoscenze	metodologie per l'organizzazione di un sistema di internal auditing, per verificare l'effettivo livello di sicurezza dei sistemi informativi 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, ecc... 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, per definire una corretta divisione delle responsabilità ed una chiara definizione delle funzioni con l'eliminazione delle possibili sovrapposizioni tipologie dei possibili attacchi al sistema informativo, per predisporre per ognuna di esse le adeguate contromisure sul piano organizzativo tecniche di backup e di restore dei sistemi informativi, per creare copie di sicurezza dalle quali recuperare i dati e ripristinare la funzionalità dei programmi in caso di incidente (per guasti, malfunzionamenti, errori,

	manomissioni, etc.)
Denominazione AdA	gestione degli aspetti legali ed amministrativi legati alla sicurezza dei sistemi informativi
Descrizione della performance	garantire il rispetto degli adempimenti previsti dalle leggi vigenti, con particolare riferimento alle norme in materia di privacy e sicurezza informatica, per minimizzare i rischi di distruzione o perdita anche accidentale dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme ai sensi del d. lgs. 196/2003 e successive modificazioni
Unità di competenza correlata	1144
Capacità	elaborare e tenere aggiornato il documento programmatico sulla sicurezza (dps) secondo le scadenze previste dal d.lgs. 196/2003 (codice sulla privacy) definire procedure tecniche conformi alle normative vigenti per consentire l'accesso ai dati da parte del titolare o del responsabile del trattamento anche in assenza degli incaricati definire un piano di formazione ed addestramento in materia di sicurezza informatica e di privacy per gli incaricati del trattamento dei dati personali, gli amministratori e gli utenti del sistema informativo minimizzare i rischi di distruzione o perdita (anche accidentale) dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme ai sensi della vigente normativa su privacy e tutela dei dati, secondo quanto stabilito dal d. lgs. 196/2003 e successive modificazioni pianificare e svolgere attività di internal auditing e verifica dell'adeguatezza delle misure di sicurezza adottate per ridurre al minimo i rischi di distruzione o perdita anche accidentale dei dati, accesso non autorizzato e trattamento non consentito o non conforme alle finalità della raccolta verificare in caso di outsourcing di parti del sistema informativo il rispetto delle norme vigenti in relazione al trattamento dei dati personali da parte dell'outsourcer
Conoscenze	misure di sicurezza obbligatorie previste dalle vigenti normative in materia di privacy, tutela dei dati personali e sicurezza informatica, per assicurare il rispetto della legge e ridurre i rischi di sanzioni penali ed amministrative normativa in materia di privacy e sicurezza dei dati personali (d. lgs 196/2003 e successive modificazioni), per aver un quadro completo degli obblighi e delle sanzioni previsti normative in materia di copyright, diritto d'autore e tutela del software, per assicurarne il rispetto nella gestione del sistema informativo tipologie di dati personali comuni e sensibili, per valutare correttamente gli obblighi previsti dalla normativa in relazione alla tipologia di dati presenti nelle varie aree del sistema informativo responsabilità civili e penali connesse alla violazione della sicurezza informatica, per valutare concretamente i rischi di sanzioni penali o amministrative legate alla gestione del sistema informativo