Responsabile dell'analisi dei rischi e della gestione e manutenzione della sicurezza di un sistema informativo (Specialista della sicurezza informatica-ICT Security Specialist)

SETTORE 14. Servizi digitali

REPERTORIO - Toscana

AdA associate alla Qualificazione

ADA.14.01.22 (ex) - Gestione della Sicurezza dell'Informazione

Tabelle di equivalenza AdA

Sezione in aggiornamento

Tabelle delle Qualificazioni dell'ADA

Qualificazioni che coprono tutti i RA dell'ADA

Qualificazione	Repertorio	RA coperti	RA1	RA2
TECNICO DELLA SICUREZZA INFORMATICA	Abruzzo	2	X	X
Esperto in sicurezza informatica	Basilicata	2	X	X
TECNICO DELLA SICUREZZA INFORMATICA	Calabria	2	X	X
TECNICO DI RETI INFORMATICHE	Emilia-Romagna	2	X	X
TECNICO DELLA SICUREZZA INFORMATICA	Emilia-Romagna	2	X	X
SPECIALISTA IN SICUREZZA INFORMATICA	Liguria	2	X	X

Qualificazione	Repertorio	RA coperti	RA1	RA2
Tecnico per la sicurezza dei sistemi informatici	Piemonte	2	X	X
Responsabile della sicurezza di reti informatiche e della protezione di dati	Puglia	2	X	X
Responsabile dell'analisi dei rischi e della gestione e manutenzione della sicurezza di un sistema informativo (Specialista della sicurezza informatica-ICT Security Specialist)	Toscana	2	X	X
Responsabile della sicurezza di reti informatiche e della protezione di dati	Toscana	2	X	X
ESPERTO IN SICUREZZA INFORMATICA	Veneto	2	X	X

Qualificazioni che coprono uno o più RA dell'ADA

Qualificazione	Repertorio	RA coperti	RA1	RA2
TECNICO SISTEMI INFORMATIVI AZIENDALI	Abruzzo	1	X	
Cybersecurity Technician	Lazio	1	X	
Tecnico della sicurezza informatica/digitale	Marche	1	X	
Tecnico gestione siti web	Sicilia	1	X	
Specialista in virtualizzazione e cloud	Umbria	1	X	
Tecnico della sicurezza dei sistemi informatici	Umbria	1	X	

Qualificazioni che coprono una o più attività dell'ADA

Qualificazione	Repertorio	RA coperti	RA1	RA2
MANAGER DELLA SICUREZZA INFORMATICA	Abruzzo	0		
Tecnico informatico	Calabria	0		
RESPONSABILE SISTEMI INFORMATIVI (BUSINESS INFORMATION MANAGER)	Lombardia	0		
RESPONSABILE DELLA SICUREZZA ICT (ICT SECURITY MANAGER)	Lombardia	0		
Tecnico informatico	Sicilia	0		
Tecnico per la sicurezza delle reti	Sicilia	0		
Tecnico installatore e manutentore di reti locali	Sicilia	0		
Tecnico dello sviluppo e gestione di prodotti e servizi digitali	Valle d'Aosta	0		

Competenze

Titolo: Gestione della sicurezza e manutenzione del sistema

Descrizione: Gestire le procedure necessarie per assicurare la sicurezza fisica e dei dati delle risorse ICT, garantendo una costante verifica ed un continuo aggiornamento delle misure adottate

Attività associate alla Competenza

Attivitá dell’ AdA ADA.14.01.22 (ex) - Gestione della Sicurezza dell'Informazione associate:

Risultato atteso:RA1: Applicare protocolli di controllo e affrontamento di

criticità relative alla sicurezza del sistema informativo, dando corso all'esecuzione di piani di ripristino in caso di crisi
Controllo sistematico degli ambienti per individuare e registrare minacce , debolezze, non conformità
Analisi degli asset critici dell'azienda per individuare vulnerabilità rispetto a intrusioni o attacchi
Applicazione di misure di affrontamento di violazioni della sicurezza secondo i protocolli
Esecuzione del piano di ripristino in caso di crisi

Risultato atteso:RA2: Implementare politiche di sicurezza informativa e tendere al loro miglioramento nel tempo anche effettuando analisi comparative e realizzando audit, test e simulazioni
Realizzazione auditing di sicurezza
Definizione di piani di ripristino
Analisi di benchmarking per il miglioramento delle procedure di gestione della sicurezza
Predisposizione e utilizzo di un risk inventory
Realizzazione di test della resilienza, anche di tipo simulativo

CONOSCENZE

Best practice e standard nella gestione della sicurezza delle informazioni
Strumenti di rafforzamento (hardening) dei servizi e dei protocolli di rete, per incrementarne la robustezza in relazione a tentativi di violazione effettivi o possibili
Tecniche di risk management, per una corretta gestione dei rischi legati alla sicurezza del sistema informativo
Tecniche di attacco e metodologie di difesa dei sistemi informativi

ABILITÀ/CAPACITÀ

Provvedere alla validazione tecnica dei tool di sicurezza
Installare le patch di aggiornamento del sistema operativo e dei vari software di protezione del sistema informativo, dopo averne verificato l'autenticità e l'integrità
Fornire raccomandazioni per applicare strategie e policy specifiche per un miglioramento continuo della sicurezza fornita
Testare periodicamente il funzionamento dei piani di ripristino, anche attraverso simulazioni di violazioni al sistema informativo
Verificare l'aggiornamento, l'efficacia e l'efficienza del software antivirus installato per la protezione del sistema informativo
Valutare le misure e gli indicatori di gestione della sicurezza in relazione alla politica aziendale
Gestire efficacemente le situazioni di crisi e di eventuali violazioni del sistema

informativo adottando le relative misure correttive
Controllare e bloccare il traffico interno ed esterno che costituisca una potenziale minaccia alla sicurezza del sistema informativo

Titolo: Progettazione ed implementazione delle misure tecniche per la sicurezza del sistema informativo

Descrizione: Progettare ed implementare le misure tecniche, relative sia alle componenti hardware che software, necessarie per assicurare al sistema informativo un adeguato livello di sicurezza

Attività associate alla Competenza

Attivitá dell' AdA ADA.14.01.22 (ex) - Gestione della Sicurezza dell'Informazione associate:

Risultato atteso:RA1: Applicare protocolli di controllo e affrontamento di criticità relative alla sicurezza del sistema informativo, dando corso all'esecuzione di piani di ripristino in caso di crisi
Controllo sistematico degli ambienti per individuare e registrare minacce , debolezze, non conformità
Analisi degli asset critici dell'azienda per individuare vulnerabilità rispetto a intrusioni o attacchi
Applicazione di misure di affrontamento di violazioni della sicurezza secondo i protocolli
Esecuzione del piano di ripristino in caso di crisi

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
Sistemi di autorizzazione degli accessi al sistema informativo
Caratteristiche e funzionalità dei proxy
Caratteristiche e funzionalità dei programmi informatici di network scanning ed intrusion detection
Caratteristiche e funzionalità dei firewall, per controllare il traffico fra due o più reti

ABILITÀ/CAPACITÀ

Contribuire alla definizione degli standard di sicurezza
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
Applicare tecniche di protezione crittografica
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 sistemi di autenticazione, autorizzazione e controllo degli accessi

Titolo: Definizione ed adozione delle misure organizzative per la sicurezza del sistema informativo

Descrizione: Definire ed adottare tutte le misure organizzative, relative sia al personale che alle infrastrutture, necessarie per garantire al sistema informativo un alto livello di sicurezza

Attività associate alla Competenza

Attivitá dell' AdA ADA.14.01.22 (ex) - Gestione della Sicurezza dell'Informazione associate:

Risultato atteso:RA2: Implementare politiche di sicurezza informativa e tendere al loro miglioramento nel tempo anche effettuando analisi comparative e realizzando audit, test e simulazioni
Realizzazione auditing di sicurezza
Definizione di piani di ripristino
Analisi di benchmarking per il miglioramento delle procedure di gestione della sicurezza
Predisposizione e utilizzo di un risk inventory
Realizzazione di test della resilienza, anche di tipo simulativo

CONOSCENZE

Tecniche di progettazione dell'organizzazione per la sicurezza, per definire una corretta divisione delle responsabilità e delle funzioni
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
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, ecc.
Normative in materia di copyright, diritto d'autore e tutela del software
Normativa in materia di privacy e sicurezza dei dati personali (D. Lgs 196/2003 e s.m.i.)
Misure di sicurezza obbligatorie previste dalle vigenti normative in materia di privacy, tutela dei dati personali e sicurezza informatica
Tipologie di attacco informatico e contromisure per evitarle
Metodologie per l'organizzazione di un sistema di internal auditing

ABILITÀ/CAPACITÀ

Elaborare i piani di Disaster Recovery e Business Continuity che, in caso di crisi, consentano 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
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 del sistema informativo per il controllo dei log, degli accessi e del traffico verso l'esterno
Programmare ed effettuare audit di sicurezza per verificare l'effettivo livello di protezione del sistema informativo
Garantire il rispetto degli adempimenti previsti dalle leggi vigenti, con particolare riferimento alle norme in materia di privacy e sicurezza informatica
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
Rispondere alle esigenze di sviluppo professionale del personale per colmare skill gaps e soddisfare le esigenze organizzative
Fornire addestramento e formazione sulla sicurezza

Titolo: Analisi dei rischi per la sicurezza del sistema informativo

Descrizione: Analizzare e valutare i rischi, le minacce e le conseguenze per la sicurezza del sistema informativo nel suo complesso e di tutte le sue componenti

Attività associate alla Competenza

Attivitá dell' AdA ADA.14.01.22 (ex) - Gestione della Sicurezza dell'Informazione associate:

Risultato atteso:RA1: Applicare protocolli di controllo e affrontamento di criticità relative alla sicurezza del sistema informativo, dando corso all'esecuzione di piani di ripristino in caso di crisi
Controllo sistematico degli ambienti per individuare e registrare minacce , debolezze, non conformità
Analisi degli asset critici dell'azienda per individuare vulnerabilità rispetto a intrusioni o attacchi
Applicazione di misure di affrontamento di violazioni della sicurezza secondo i protocolli
Esecuzione del piano di ripristino in caso di crisi

Risultato atteso:RA2: Implementare politiche di sicurezza informativa e tendere al loro miglioramento nel tempo anche effettuando analisi comparative e realizzando audit, test e simulazioni
Realizzazione auditing di sicurezza
Definizione di piani di ripristino
Analisi di benchmarking per il miglioramento delle procedure di gestione della sicurezza
Predisposizione e utilizzo di un risk inventory
Realizzazione di test della resilienza, anche di tipo simulativo

CONOSCENZE

Tipologia delle potenziali minacce all'integrità, riservatezza e disponibilità delle informazioni e delle risorse di un sistema informativo o di una rete
Tecniche di attacco informatico e relative contromisure
Principi di sicurezza delle basi di dati
Metodologie di analisi dei rischi per la sicurezza di un sistema informativo
Principi di sicurezza dei sistemi informativi
Architettura hardware e software dei sistemi di elaborazione elettronica, con particolare riferimento ai punti di forza e di debolezza in relazione alle esigenze

di sicurezza e protezione dei dati

ABILITÀ/CAPACITÀ

Valutare rischi, minacce e conseguenze
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 un documento con la valutazione dei rischi per la sicurezza del sistema informativo, contenente l'analisi delle minacce e delle vulnerabilità individuate e delle possibili contromisure
Analizzare gli aspetti critici del sistema informativo per identificare debolezze e vulnerabilità riguardo a possibili intrusioni o attacchi

Codici ISTAT CP2021 associati

Codici ISTAT ATECO associati

Codice Ateco	Titolo Ateco
62.01.00	Produzione di software non connesso all'edizione
62.02.00	Consulenza nel settore delle tecnologie dell'informatica
62.03.00	Gestione di strutture e apparecchiature informatiche hardware - housing (esclusa la riparazione)
62.09.09	Altre attività dei servizi connessi alle tecnologie dell'informatica nca
63.11.20	Gestione database (attività delle banche dati)
63.11.30	Hosting e fornitura di servizi applicativi (ASP)
63.12.00	Portali web

Istituto Nazionale per l’Analisi delle Politiche Pubbliche - Corso d’Italia, 33 - 00198 Roma - C.F. 80111170587