concorsi superiori

Concorso RIPAM

178 Area Funzionari ed Elevata qualificazione dei Piccoli Comuni

32 Funzionari con competenze digitali

MANUALE di TEORIA e QUIZ per la prova scritta

NLD CONCORSI

Cybersecurity Act, che istituisce il sistema europeo di certificazione della cybersicurezza. Tra le sue competenze rientrano l'**accreditamento degli organismi di valutazione della conformità** e la supervisione sul rilascio dei **certificati europei di sicurezza cibernetica**, come previsto dall'art. 7, comma 1, lett. e, del Decreto-Legge 14 giugno 2021, n. 82.
L'ACN, nell'ambito di tali attività, delega specifici compiti di certificazione al **Ministero della Difesa** e al **Ministero dell'Interno**, ciascuno in relazione alle rispettive aree di competenza, ai sensi dell'art. 7, comma 1, lett. e, punti 1-2. Questa struttura di delega e supervisione garantisce un'efficace gestione delle attività di certificazione, contribuendo al consolidamento della sicurezza cibernetica a livello nazionale ed europeo.

► 2.1.3. Protezione delle infrastrutture critiche.

L'**Agenzia per la Cybersicurezza Nazionale (ACN)** ha assunto le funzioni precedentemente attribuite al **Ministero dello Sviluppo Economico** in materia di sicurezza delle **infrastrutture critiche**, incluse le competenze relative al **Perimetro di sicurezza nazionale cibernetica**, come previsto dall'art. 7, comma 1, lett. f, h, i, del Decreto-Legge 14 giugno 2021, n. 82.
Tali funzioni comprendono la **valutazione delle infrastrutture strategiche**, lo svolgimento delle **attività ispettive**, l'**accertamento delle violazioni** e l'**irrogazione delle sanzioni** connesse. Questo trasferimento di competenze mira a consolidare un approccio integrato e centralizzato alla sicurezza cibernetica delle infrastrutture strategiche, rafforzando così la capacità di prevenzione e gestione delle minacce informatiche.

► 2.1.4. Sviluppo di capacità crittografiche e promozione della sicurezza

L'ACN promuove lo sviluppo di capacità crittografiche nazionali attraverso il **Centro nazionale di crittografia**, istituito per migliorare la sicurezza dei sistemi informativi e favorire l'adozione di tecnologie blockchain come strumento di cybersicurezza (art. 7, comma 1, lett. m-bis).
L'Agenzia collabora con centri universitari e di ricerca per lo sviluppo di algoritmi crittografici proprietari, contribuendo alla crescita dell'autonomia tecnologica del Paese.

► 2.1.5. Formazione e sensibilizzazione.

Tra le funzioni attribuite all'**Agenzia per la Cybersicurezza Nazionale (ACN)** rientra la **promozione della cultura della cybersicurezza**, come previsto dall'art. 7, comma 1, lett. u e v, del Decreto-Legge 14 giugno 2021, n. 82. A tal fine, l'Agenzia sviluppa programmi formativi, organizza campagne di sensibilizzazione e realizza attività di divulgazione, con l'obiettivo di accrescere la consapevolezza e la preparazione in materia di sicurezza cibernetica.
L'ACN sostiene, inoltre, percorsi accademici dedicati, favorendo l'istituzione di **borse di studio** e programmi di **dottorato** in ambito cibernetico, contribuendo così alla formazione di competenze altamente specializzate, essenziali per affrontare le sfide poste dalle minacce informatiche.

► 2.1.6. Cooperazione internazionale.

L'**Agenzia per la Cybersicurezza Nazionale (ACN)** è incaricata di promuovere e gestire la **cooperazione con enti e istituzioni internazionali**, tra cui l'**Agenzia europea per la cybersicurezza (ENISA)**, come stabilito dall'art. 7, comma 1, lett. q, del Decreto-Legge 14 giugno 2021, n. 82.
Nell'esercizio di tale funzione, l'ACN rappresenta l'Italia nelle sedi internazionali, assicurando il **raccordo tra le politiche nazionali** e le strategie globali in materia di cybersicurezza. Questo ruolo permette di rafforzare il contributo italiano alla definizione di politiche condivise e di favorire una maggiore integrazione con le iniziative europee e internazionali.

► 2.2. La Direttiva NIS2 e gli strumenti nazionali di cybersicurezza

L'**Agenzia per la Cybersicurezza Nazionale (ACN)** ha sviluppato e implementato una gamma di strumenti e iniziative mirate a potenziare la sicurezza informatica nell'ambito della **PA** italiana. Queste misure si inseriscono in un quadro di interventi coordinati, volti a garantire la protezione delle

infrastrutture critiche, la prevenzione degli incidenti cibernetici e la resilienza complessiva dei sistemi informatici utilizzati dalle amministrazioni pubbliche, in linea con le disposizioni normative e strategiche nazionali.
La **Direttiva (UE) 2022/2555**, nota come **NIS2**, ha rafforzato il quadro europeo in materia di **cybersicurezza**, sostituendo la precedente **Direttiva NIS** e ampliando il numero dei soggetti pubblici e privati tenuti ad adottare misure di sicurezza informatica. Essa mira ad assicurare un **livello comune elevato di protezione delle reti e dei sistemi informativi** nell'Unione europea, imponendo obblighi in materia di **gestione del rischio**, **prevenzione degli incidenti**, **continuità operativa**, **sicurezza della catena di approvvigionamento** e **notifica degli incidenti significativi**. In Italia, la direttiva è stata recepita con il **D.Lgs. 4 settembre 2024, n. 138**, che attribuisce un ruolo centrale all'**Agenzia per la Cybersicurezza Nazionale** e rafforza gli strumenti di **cooperazione**, **monitoraggio** e **condivisione delle informazioni** tra soggetti pubblici e privati.

► 2.2.1. Il CSIRT Italia.

Il ***Computer Security Incident Response Team*** **- Italia** (CSIRT **I**talia), istituito presso l'**Agenzia per la Cybersicurezza Nazionale** (ACN), costituisce il principale organismo operativo per la gestione e la prevenzione degli **incidenti di sicurezza informatica** a livello nazionale. La sua istituzione è frutto di un processo di riorganizzazione che ha accorpato le funzioni in precedenza svolte dal CERT-PA e dal CERT Nazionale. Il CSIRT opera nel quadro normativo delineato dal **D.Lgs. 18 maggio 2018, n. 65** (Direttiva NIS) e dal **D.L. 14 giugno 2021, n. 82**.
La principale missione del CSIRT consiste nel garantire un'efficace prevenzione e gestione delle minacce cibernetiche, nonché nel promuovere un approccio coordinato alla sicurezza informatica a livello nazionale. Sul piano operativo, il CSIRT fornisce supporto tecnico per affrontare gli incidenti informatici, pubblica avvisi relativi a vulnerabilità critiche e contribuisce alla circolazione di informazioni strategiche per il contrasto alle minacce emergenti. In tal senso, agisce come **punto di contatto nazionale** per la notifica di incidenti rilevanti da parte di soggetti pubblici e privati, in particolare per quelli ricompresi nel **Perimetro di Sicurezza Nazionale Cibernetica**.
L'attività del CSIRT si distingue per la sua capacità di analizzare tempestivamente flussi di dati informatici, individuando in anticipo le minacce potenziali e facilitando la diffusione di dati utili all'identificazione di vulnerabilità. Inoltre, esso promuove la **consapevolezza sui rischi cibernetici** attraverso la pubblicazione di rapporti tecnici e linee guida, con particolare attenzione ai professionisti del settore IT e ai decisori istituzionali.
A livello internazionale, il CSIRT Italia opera in stretto coordinamento con organismi europei, come la rete CSIRT dell'Unione Europea istituita dalla **Direttiva NIS2**, e con enti quali l'**Agenzia Europea per la Cybersicurezza (ENISA)** e la **NATO**, consolidando strategie condivise per la protezione delle infrastrutture critiche.
Dal punto di vista strutturale, il CSIRT Italia funge da perno per una rete di CSIRT settoriali, concepiti per rispondere alle esigenze specifiche di ambiti come energia, sanità e telecomunicazioni, assicurando così una copertura capillare e settorializzata nella gestione della sicurezza cibernetica.
Le attività svolte dal CSIRT Italia rivestono un'importanza strategica nella riduzione dei tempi di risposta agli incidenti e nel miglioramento della **resilienza informatica nazionale**. Attraverso la sua azione di prevenzione, gestione e coordinamento, il CSIRT contribuisce in modo determinante alla tutela delle infrastrutture critiche e alla sicurezza delle informazioni sensibili, consolidandosi quale elemento cardine della strategia nazionale di cybersicurezza.

► 2.2.2. La Piattaforma Nazionale di Condivisione delle Informazioni sulla Cybersecurity.

La **Piattaforma Nazionale di Condivisione delle Informazioni sulla Cybersecurity**, istituita dall'**Agenzia per la Cybersicurezza Nazionale** (ACN), rappresenta uno strumento essenziale per promuovere la cooperazione e lo scambio di informazioni in materia di sicurezza informatica tra organizzazioni pubbliche e private. Tale piattaforma è stata introdotta in conformità al **Decreto Legislativo 4 settembre 2024, n. 138**, che recepisce la **Direttiva (UE) 2022/2555** (NIS2), con l'obiettivo di assicurare un livello uniforme ed elevato di protezione delle reti e dei sistemi informativi su scala nazionale.
A decorrere dal **1° dicembre 2024** e fino al **28 febbraio 2025**, tutte le **medie e grandi imprese**, con l'inclusione, in alcuni casi specifici, anche di **piccole e microimprese**, nonché le **Pubbliche**

Amministrazioni soggette alla normativa, hanno l'obbligo di registrarsi sulla piattaforma tramite il portale servizi dell'ACN. Tale registrazione costituisce il primo passaggio di un percorso di collaborazione che, a partire da **aprile 2025**, sarà finalizzato al rafforzamento della sicurezza informatica sia a livello nazionale che europeo.
La piattaforma non si limita a facilitare la comunicazione diretta tra l'ACN e i soggetti registrati, ma svolge un ruolo cruciale nella condivisione di **best practice**, informazioni su **minacce emergenti** e **vulnerabilità**, favorendo una risposta più coordinata ed efficace agli incidenti di sicurezza informatica.
Parallelamente, essa offre un supporto significativo alle organizzazioni nell'adempimento degli obblighi normativi, fornendo strumenti specifici per la **gestione del rischio** e la **notifica degli incidenti**, in linea con le nuove disposizioni legislative.
Attraverso tali funzionalità, la piattaforma si configura come un elemento centrale della strategia nazionale di cybersicurezza, promuovendo una sinergia tra soggetti pubblici e privati per affrontare con maggiore efficacia le sfide poste dall'evoluzione delle minacce cibernetiche.
La piattaforma si colloca nell'ambito della realizzazione dello ***European Cybershield***, previsto dalla "**EU *Cybersecurity Strategy for Digital Decade***", il cui obiettivo consiste nella creazione di una rete europea di ***Information Sharing and Analysis Centers*** **(ISAC)** e di **Security Operations Centers (SOC)**. In tale contesto, l'**ISAC Italia**, istituito presso l'**Agenzia per la Cybersicurezza Nazionale** (ACN), svolge il ruolo di **Centro nazionale** per l'analisi e la condivisione di informazioni in ambito cibernetico.
L'ISAC Italia facilita la costituzione di ISAC settoriali e offre servizi di **analisi**, ***capacity building*** e **info-sharing** attraverso canali sicuri e riservati, garantendo un elevato livello di protezione delle informazioni scambiate. Questa struttura si pone l'obiettivo di promuovere la **cooperazione** tra stakeholder omogenei, incentivando la condivisione di informazioni su **minacce**, **vulnerabilità** e **lezioni apprese**. In tal modo, contribuisce a ridurre le discrepanze tra i diversi livelli di maturità nella gestione dei rischi e delle minacce informatiche, rafforzando la resilienza complessiva del sistema nazionale.
L'implementazione dell'ISAC Italia rappresenta un'applicazione concreta della misura **#34 della Strategia Nazionale di Cybersicurezza**, che riceve finanziamenti attraverso l'investimento **1.5 "Cybersecurity"** previsto dal **Piano Nazionale di Ripresa e Resilienza (PNRR)**. Questo approccio integrato riflette l'impegno del Paese nel contribuire alla costruzione di una rete di cooperazione europea in grado di affrontare in modo coordinato le sfide poste dalla crescente complessità delle minacce cibernetiche.

► 2.2.3. Linee Guida e framework per la sicurezza informatica.

L'**Agenzia per la Cybersicurezza Nazionale (ACN)** ha predisposto una serie di **linee guida** e **framework** finalizzati a supportare le organizzazioni italiane nell'adozione di misure efficaci di **sicurezza informatica**. Tra questi spicca il **Framework Nazionale per la Cybersecurity e la Data Protection**, ispirato al modello statunitense del **National Institute of Standards and Technology (NIST)**. Tale framework rappresenta uno strumento operativo che consente di organizzare e gestire i processi di cybersecurity, risultando adattabile sia ad **enti pubblici** sia a **soggetti privati**, indipendentemente dalle loro dimensioni. Per facilitarne l'adozione, l'ACN ha reso disponibile il **Cyber Security Framework Tool**, un insieme di strumenti utili alla contestualizzazione e implementazione delle misure previste dal framework.
In attuazione dell'articolo 8 della **legge n. 90/2024**, l'ACN ha pubblicato le **Linee guida per il rafforzamento della resilienza**, destinate ai soggetti pubblici, al fine di orientarne l'adozione di misure di sicurezza volte a migliorare la **resilienza cibernetica**. Ulteriormente, la **Guida alla notifica degli incidenti al CSIRT Italia** fornisce un riferimento operativo dettagliato sulla procedura di segnalazione degli **incidenti informatici**, elemento essenziale per garantire la sicurezza delle reti e dei sistemi informativi.
Al fine di promuovere una terminologia condivisa, l'ACN ha introdotto la **tassonomia cyber (TC-ACN)**, un lessico comune pensato per agevolare lo scambio di informazioni a livello nazionale. Questa tassonomia mira a standardizzare la descrizione e la condivisione degli eventi cibernetici, oltre a uniformare le notifiche di incidenti al **CSIRT Italia**.
Le iniziative promosse dall'ACN evidenziano un impegno costante nel fornire strumenti e orientamenti pratici, finalizzati al rafforzamento della sicurezza informatica. Attraverso l'adozione di approcci coordinati e standardizzati, l'agenzia contribuisce alla diffusione di una cultura della **cybersicurezza** e