concorsi superiori

Concorso MINISTERO della CULTURA

1.800 Assistenti

300 Assistenti tecnici per la tutela e la valorizzazione (Cod. 02)

MANUALE di TEORIA e QUIZ per la prova scritta

NLD CONCORSI

©NLD Concorsi

consapevolezza in merito ai **rischi informatici** e promuovere comportamenti conformi alle **best practice di sicurezza**, in linea con il già analizzato art. 13, comma 1. Tale attività formativa risulta indispensabile per garantire un utilizzo appropriato degli strumenti informatici da parte del personale, nonché per assicurare la conoscenza delle politiche di sicurezza adottate dall'ente e delle procedure operative da seguire in caso di incidenti. L'obiettivo è quello di creare una cultura della sicurezza all'interno delle amministrazioni pubbliche, riducendo il rischio umano quale fattore critico negli attacchi informatici.
Infine, l'elaborazione di **piani di *disaster recovery*** e di ***business continuity*** costituisce una misura essenziale per la resilienza operativa delle pubbliche amministrazioni. I piani di *disaster recovery* delineano le procedure necessarie per il ripristino dei sistemi e dei dati in seguito a disastri o incidenti che compromettano la funzionalità dell'infrastruttura informatica. Parallelamente, i piani di business *continuity* sono finalizzati a garantire la continuità delle attività operative dell'ente, anche in presenza di interruzioni significative dei servizi. Entrambi gli strumenti si configurano come parte integrante di una strategia di sicurezza volta a ridurre al minimo l'impatto di eventi critici, assicurando la capacità dell'amministrazione di proseguire nello svolgimento delle proprie funzioni essenziali.

► 1.3.2. Misure reattive.

Le **misure reattive** assumono un ruolo essenziale nella gestione degli **incidenti di sicurezza informatica** all'interno della Pubblica Amministrazione (PA), assicurando una risposta pronta ed efficace alle minacce emergenti. Tali misure si fondano su due ambiti operativi distinti.
In primo luogo, le **procedure di *incident response*** si sviluppano attraverso un processo strutturato, articolato in fasi operative progressive. Esse includono la **rilevazione**, consistente nel monitoraggio continuo per individuare tempestivamente eventi anomali o sospetti, seguita dall'**analisi**, che mira a una valutazione approfondita della natura e dell'impatto dell'incidente. A queste si aggiungono il **contenimento e la mitigazione**, che implicano l'adozione di interventi immediati volti a limitare i danni e prevenire ulteriori compromissioni. Successivamente, si procede al **ripristino**, con la riparazione dei sistemi e la ripresa delle normali operazioni, assicurandosi che le vulnerabilità sfruttate siano state eliminate. Infine, la fase **post-incidente** prevede la documentazione degli eventi, l'analisi delle lezioni apprese e l'aggiornamento delle misure di sicurezza al fine di ridurre il rischio di incidenti futuri. Un apporto rilevante a questo processo è dato dall'**Agenzia per la Cybersicurezza Nazionale (ACN)**, che, attraverso la pubblicazione della "Guida alla notifica degli incidenti al CSIRT Italia", fornisce un quadro procedurale articolato in quattro fasi, utile per consentire alle amministrazioni di comunicare efficacemente l'impatto di un evento al ***Computer Security Incident Response Team*** **(CSIRT)**, potenziando la capacità di risposta collettiva.
In secondo luogo, la **collaborazione con il CSIRT Italia**, istituito all'interno dell'ACN, rappresenta un elemento strategico nella gestione degli incidenti di sicurezza. Le Pubbliche Amministrazioni hanno l'obbligo di notificare con tempestività tali eventi, conformandosi alle linee guida predisposte, così da garantire una risposta **coordinata ed efficace**. Tale collaborazione favorisce anche lo scambio di informazioni relative a minacce e vulnerabilità, contribuendo ad accrescere la **resilienza** del sistema digitale nazionale.
L'implementazione di queste misure reattive, in ossequio alle disposizioni normative vigenti, risulta indispensabile per la tutela delle **infrastrutture critiche** della PA e per la salvaguardia dei dati personali dei cittadini.

2. Il ruolo dell'Agenzia per la Cybersicurezza Nazionale (ACN)

Prima dell'istituzione dell'**Agenzia per la Cybersicurezza Nazionale (ACN)**, la gestione della sicurezza cibernetica in Italia risultava frammentata tra una pluralità di enti e istituzioni. Le competenze in materia di protezione delle **infrastrutture critiche** e di risposta agli **incidenti informatici** erano ripartite tra il **Dipartimento delle Informazioni per la Sicurezza (DIS)**, l'**Agenzia per l'Italia Digitale (AgID)** e il **Ministero dello Sviluppo Economico (MISE)**. Tale frammentazione ostacolava l'elaborazione di una strategia unitaria ed efficace per fronteggiare le minacce cibernetiche, in un contesto caratterizzato da una crescente complessità.
L'esigenza di un approccio maggiormente coordinato e centralizzato è divenuta sempre più

ONLINE ACCESS

evidente negli ultimi anni, in concomitanza con l'aumento esponenziale degli **attacchi informatici** e con la crescente dipendenza delle attività sociali ed economiche dalle tecnologie digitali. Di fronte a queste sfide, il Governo italiano ha avvertito la necessità di riorganizzare l'architettura nazionale di cybersicurezza, dando vita all'**ACN** mediante il **Decreto-Legge 14 giugno 2021, n. 82**, successivamente convertito, con modificazioni, dalla **Legge 4 agosto 2021, n. 109**.

► 2.1. Compiti e funzioni dell'ACN.

L'**Agenzia per la Cybersicurezza Nazionale (ACN)**, istituita dal **Decreto-Legge 14 giugno 2021, n. 82**, convertito con modificazioni dalla **Legge 4 agosto 2021, n. 109**, è stata designata quale **Autorità nazionale per la cybersicurezza**. La sua missione comprende la **protezione delle infrastrutture critiche** e il **coordinamento delle politiche nazionali di sicurezza cibernetica**, contribuendo a rafforzare la resilienza del sistema Paese. Le funzioni dell'Agenzia sono dettagliatamente delineate all'art. 7 del decreto, che ne definisce il perimetro operativo. L'ACN svolge le proprie attività in stretta collaborazione con le **istituzioni pubbliche** e con gli **operatori privati**, promuovendo una sinergia indispensabile per affrontare le sfide connesse alla sicurezza cibernetica in un contesto nazionale e globale sempre più interconnesso. L. 23 settembre **2025**, n. 132 (**Legge quadro sull'Intelligenza artificiale**) affida all'**Agenzia per l'Italia digitale** (**AgID**) e l'**Agenzia per la cybersicurezza nazionale** (**ACN**) il compito di dare attuazione, in Italia, alle regole sull'IA previste sia a livello nazionale sia dall'Unione europea, fermi i poteri della Banca d'Italia, della CONSOB e dell'IVASS come autorità di vigilanza del mercato, secondo quanto stabilito dall'AI Act. In particolare, l'AgID è responsabile di **promuovere l'innovazione** e lo **sviluppo dell'intelligenza artificiale**, definire le **procedure** e a **esercitare** le **funzioni** e i **compiti in materia di notifica**, **valutazione**, **accreditamento** e monitoraggio dei soggetti incaricati di verificare la conformità dei sistemi di intelligenza artificiale, secondo quanto previsto dalla normativa nazionale e dell'Unione europea; l'**ACN**, anche ai fini di assicurare la tutela della cybersicurezza, è responsabile per la **vigilanza**, ivi incluse le **attività ispettive** e **sanzionatorie**, dei sistemi di intelligenza artificiale, secondo quanto previsto dalla normativa nazionale e dell'Unione europea. L'ACN è altresì responsabile per la promozione e lo sviluppo dell'intelligenza artificiale relativamente ai profili di cybersicurezza. L'AgID e l'ACN, ciascuna per quanto di rispettiva competenza, assicurano l'istituzione e la gestione congiunta di spazi di sperimentazione finalizzati alla realizzazione di sistemi di intelligenza artificiale conformi alla normativa nazionale e dell'Unione europea, sentiti il Ministero della difesa per gli aspetti relativi ai sistemi di intelligenza artificiale impiegabili in chiave duale e il Ministero della giustizia per i modelli e i sistemi di intelligenza artificiale applicabili all'attività giudiziaria.

► 2.1.1. Coordinamento e resilienza cibernetica.

L'**Agenzia per la Cybersicurezza Nazionale (ACN)** garantisce il coordinamento tra i soggetti pubblici competenti in materia di **cybersicurezza**, promuovendo azioni comuni volte ad assicurare la **resilienza cibernetica** delle **infrastrutture strategiche** e a sostenere lo sviluppo digitale del Paese, in conformità a quanto previsto dall'art. 7, comma 1, lett. a, del Decreto-Legge 14 giugno 2021, n. 82. Tra i suoi compiti figura altresì la promozione dell'**autonomia tecnologica** nazionale ed europea, con un'attenzione particolare ai prodotti e ai processi informatici di rilevanza strategica.
L'Agenzia intrattiene rapporti diretti con il **Ministero dell'Interno**, che mantiene il ruolo di autorità nazionale di pubblica sicurezza, e con l'**Ufficio centrale per la segretezza**, competente per le reti e i sistemi classificati, come stabilito dal medesimo art. 7, comma 1, lett. a.
Uno dei compiti principali dell'ACN è rappresentato dall'elaborazione e dall'aggiornamento della **Strategia nazionale di cybersicurezza**, ai sensi dell'art. 7, comma 1, lett. b. Tale strategia definisce le linee guida e gli obiettivi di medio e lungo termine necessari per rafforzare la **resilienza cibernetica** del sistema Paese. Essa comprende iniziative mirate alla prevenzione, gestione e risposta alle **minacce informatiche**, costituendo uno strumento essenziale per affrontare le sfide connesse alla sicurezza cibernetica in un contesto sempre più interconnesso.

► 2.1.2. Certificazione della cybersicurezza.

In qualità di **Autorità nazionale di certificazione della cybersicurezza**, l'**Agenzia per la Cybersicurezza**

Nazionale (ACN) è incaricata dell'attuazione del **Regolamento (UE) 2019/881**, noto come **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. Strumenti e iniziative dell'ACN

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

©NLD Concorsi