Obiettivi d'esame IC DAC 2.0

Amministrazione Digitale

Il Codice dell'Amministrazione digitale (CAD)

- *Comprendere i concetti di e-Governament, Amministrazione digitale, dematerializzazione documentale, documento elettronico. Il Codice dell'Amministrazione Digitale (CAD)*
- *Comprendere le differenze fra i diversi tipi di documento informatico. Documento informatico, documento analogico, copia informatica di documento analogico copia per immagine su supporto informatico di documento analogico, copia informatica di documento informatico, duplicato informatico, copia analogica di documento informatico. Timbro digitale (glifo). Il Quick Response Code (QR Code). La Gazzetta Ufficiale Certificata.*
- *Essere consapevoli che l'Amministrazione digitale cambierà radicalmente gli strumenti di lavoro e il modo di lavorare in un contesto di processi amministrativi completamente riprogettati.*
- *Riconoscere gli obblighi della PA e i diritti digitali dei cittadini e delle imprese. Le carte elettroniche e i siti web della PA. Sicurezza, continuità operativa e "disaster recovery".*
- *Riconoscere la portata della rivoluzione digitale che coinvolge: firma digitale, posta elettronica certificata, protocollo elettronico, fatturazione elettronica, conservazione sostitutiva.*

Definizioni, finalità e ambito di applicazione del CAD

- *Comprendere il ruolo del Certificatore. Il certificato elettronico, il certificato qualificato.*
- *Comprendere il concetto di autenticazione informatica; documento informatico; gestione informatica del documento. Il valore giuridico del documento informatico.*

Firma Digitale (FD)

Soggetti e oggetti della firma digitale

- *Comprendere l'importanza della crittografia; le chiavi crittografiche simmetriche e asimmetriche, la coppia di chiavi pubblica e privata.*
- *Comprendere caratteristiche e utilità della funzione di Hash e dell'impronta digitale. Il non ripudio.*

- *Riconoscere i differenti dispositivi di firma: smart card, token USB; il Secure Signature Creation Device (SSCD); i dispositivi di firma remota (HSM); il tablet di firma (firma grafometrica).*
- *Riconoscere le differenti tipologie di firme e la loro efficacia giuridica: firma elettronica, avanzata, qualificata, autenticata, digitale; forte e debole.*
- *Riconoscere le funzioni dell'Agenzia per l'Italia Digitale, dei Certificatori, dei Certificatori qualificati e dei Certificatori accreditati. La responsabilità civile del Certificatore.*

Aspetti giuridici

- *Riconoscere l'uso inappropriato della firma digitale; la sottoscrizione digitale equivalente a quella autografa e il processo di autenticazione. Il potere di firma nel documento informatico e l'uso della firma digitale nella PA.*
- *Comprendere le differenti caratteristiche delle varie firme elettroniche in giudizio: il valore probatorio della firma digitale e il valore probante delle firme deboli*
- *Comprendere il valore legale della firma digitale, il disconoscimento della firma digitale.*
- *Comprende le caratteristiche di validità temporale della firma digitale. Il servizio di marcatura temporale e metodi equivalenti per ottenere una marcatura temporale opponibile a terzi.*
- *Riconoscere le vulnerabilità della firma digitale: la sicurezza del processo di firma, i documenti contenenti macro e codice eseguibile.*

Aspetti tecnologici

- *Riconoscere e utilizzare i vari formati di firma digitale: formato pkcs#7 (p7m), formato PDF, formato XML. Le firme multiple; il WYSIWYS.*
- *Essere in grado di attrezzarsi per la firma digitale. L'elenco dei Certificatori. L'importanza del Manuale operativo specifico di ciascun Certificatore.*

Operare con le firme digitali

- *Essere in grado di apporre e verificare la firma di un documento in formato pkcs#7 (p7m). La verifica di validità dei certificati scaduti, sospesi e dipendenti dal contenuto del documento. Essere in grado di verificare una firma digitale operando con i software e con i servizi on-line disponibili sui siti web degli Enti Certificatori.*
- *Essere in grado di apporre firme ed effettuare verifiche utilizzando il formato PDF.*
- *Essere in grado di apporre una marca temporale a un documento informatico che contiene un insieme di impronte.*

Posta Elettronica Certificata (PEC)

Caratteristiche della PEC

- *Comprendere che la PEC è un sistema di posta elettronica che dà prova opponibile a terzi dell'invio e della consegna del messaggio, genera enormi risparmi economici e semplifica i rapporti tra privati e tra questi e la PA. Lo scambio tra applicazioni.*
- *Riconoscere l'estrema affidabilità della PEC in quanto conta sui livelli minimi di servizio garantiti dalla norma, sul Manuale operativo e sui servizi aggiuntivi resi disponibili dal gestore prescelto.*
- *Comprendere i ruoli degli attori della PEC: mittente, destinatario, gestori, rete di comunicazione, oggetto dell'invio. Le ricevute, gli avvisi e le buste.*
- *Comprendere che la PEC è un sistema di trasporto. L'uso appropriato della PEC; l'archiviazione e la ricerca dei messaggi e delle ricevute; il file di log.*
- *Riconoscere i punti di forza della PEC: trasmissione di qualsiasi contenuto digitale; semplicità ed economicità di trasmissione, inoltro, riproduzione, archiviazione e ricerca; invio multiplo; velocità di consegna; accesso da qualsiasi locazione; elevati requisiti di qualità e continuità del servizio; garanzia di sicurezza e privacy.*
- *Comprendere che il valore legale del messaggio di PEC è salvaguardato esclusivamente nel caso di trasmissione tra caselle di PEC.*
- *Comprendere che per la PA l'utilizzo della PEC è allo stesso tempo una opportunità e un obbligo. Il domicilio digitale del cittadino. L'Anagrafe Nazionale della Popolazione Residente (ANPR).*
- *Comprendere i limiti della PEC. Le alternative alla PEC; i certificati S/MIME, la REM e la casella di posta elettronica CEC-PAC.*

Operare con la PEC

- *Essere in grado di configurare il proprio account di PEC e il proprio client di posta elettronica.*
- *Conoscere tutti i passi operativi per l'invio e la lettura di un messaggio di PEC ed essere in grado di svolgerli praticamente.*
- *Riconoscere gli obblighi e le responsabilità del Gestore e del Titolare del servizio di PEC.*

Siti web delle PA. Sicurezza, continuità operativa e "disaster recovery", cloud computing

Essere in grado di riconoscere l'importanza della comunicazione erogata attraverso i siti web delle Pubbliche Amministrazioni

- *Conoscere gli obblighi cui sono sottoposti i siti web delle Pubbliche amministrazioni. Caratteristiche, contenuti, finalità della web communication.*
- *Comprendere l'importanza del customer satisfaction dell'utenza finale.*
- *Conoscere i principi esposti nelle "Linee Guida per i siti web delle PA" provvedute dall'Agenzia per l'Italia Digitale.*

Sicurezza

- *Comprendere l'importanza fondamentale della sicurezza informatica e della protezione dei dati immateriali.*
- *Essere consapevoli dell'importanza strategica della protezione cibernetica delle infrastrutture critiche.*

Continuità operativa e "disaster recovery"

- *Conoscere gli obblighi imposti relativi alla continuità operativa e disaster recovery. Distinguere i diversi parametri (RTO e RPO) e modalità del disaster recovery (modalità sincrona, asincrona e mista).*
- *Essere in grado di reperire lo studio di fattibilità tecnica del piano di continuità operativa ed il tool di autovalutazione provveduti dell'Agenzia per l'Italia Digitale.*

Cloud computing

- *Comprendere l'importanza di servizi e vantaggi ottenibili in modalità cloud computing.*
- *Comprendere rischi e vantaggi legati alla modalità operativa in cloud computing.*