Codice dell'Amministrazione Digitale
Obiettivi e contenuti del corso

Modulo 1: Amministrazione Digitale (CAD)

Il Codice dell'Amministrazione Digitale

Il Codice dell'Amministrazione Digitale: cosa è? Perché?

Comprendere i concetti di e-Government, Amministrazione digitale, dematerializzazione documentale, documento elettronico. Distinguere le differenze fra i diversi tipi di documento informatico e come si producono (D. Lgs. 26 agosto 2016 n. 179). Essere consapevoli che l'Amministrazione digitale cambierà rapidamente e radicalmente strumenti di lavoro e modalità operative 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. Riconoscere la portata della rivoluzione digitale che coinvolge: firma digitale, posta elettronica certificata, protocollo elettronico, fatturazione elettronica, conservazione sostitutiva, riversamenti diretti o indiretti.

- *documento analogico*
- *documento informatico*
- *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.*
- *Il timbro digitale (glifo). La Gazzetta Ufficiale Certificata. Cosa è, a cosa serve, come si decodifica.*
- *Il QR Code: cosa è, come si produce, possibili applicazioni*
- *Prove pratiche di produzione delle diverse tipologie di documenti informatici*
- *Prove pratiche di decodifica di timbri digitali con tecniche on line e off line*
- *Prove pratiche di realizzazione di QR Code*

Modulo 2: Firma Digitale (FD)

Soggetti e oggetti della firma digitale. Aspetti operativi.

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 (forti e deboli.). Il non ripudio. Il sigillo elettronico.

Comprendere le caratteristiche della funzione di Hash e dell'impronta del documento.

Comprendere l'importanza della crittografia per la protezione della documentazione confidenziale; le chiavi crittografiche simmetriche e asimmetriche, la coppia di chiavi pubblica e privata. Conoscere le vulnerabilità della firma digitale: la sicurezza del processo di firma, i documenti contenenti macro e codice eseguibile.
Riconoscere e utilizzare i vari formati di firma digitale. Essere in grado di attrezzarsi per operare con la firma digitale. L'Agenzia per l'Italia Digitale. L'elenco dei Certificatori. L'importanza del Manuale operativo specifico di ciascun Certificatore. 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. Comprendere le caratteristiche di validità temporale della firma digitale. Il servizio di marcatura temporale e metodi equivalenti per ottenere una marcatura temporale opponibile a terzi.

- *Prove pratiche di apposizione e verifica di autenticità e non manipolazione della firma digitale (CaDES, PaDES, XaDES) con uso di strumenti reali operando con i software ed i servizi on line disponibili sui siti web degli Enti Certificatori.*
- *Prove pratiche di crittografia/decrittografia con uso di free software PGP*
- *Prove pratiche di calcolo dell'impronta del file con i diversi algoritmi (SHA-1, SHA-256, MD5) e ricalcolo ai fini della verifica di non alterazione del file con uso di free software on line e off line.*

Modulo 3: Posta Elettronica Certificata, Fatturazione Elettronica, Identità Digitale

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.
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. Comprendere i limiti della PEC. Le alternative alla PEC. Operare con la PEC. Essere in grado di configurare il proprio account di PEC.

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. I servizi equivalenti in Europa.

- *Prove pratiche su come ottenere un account PEC. Configurazione del servizio.*
- *Invio e ricezione con strumenti autentici (PEC)*

Il domicilio digitale del cittadino e l'Anagrafe Nazionale della Popolazione Residente (ANPR). L'Anagrafe Italiana Residenti Estero (AIRE). L'Anagrafe Nazionale dei Numeri Civici e delle Strade Urbane (ANNCSU). L'Indice delle Pubbliche Amministrazioni (IPA). Sistema di interscambio (SdI). Sistema Pubblico per la gestione dell'Identità Digitale (SPID). PagoPA, Prestatori di Servizi di Pagamento (PSP). La marca da bollo digitale.

Modulo 4: Siti web delle PA. Cyber Security. Continuità operativa e "disaster recovery". Cloud computing. Opportunità e rischi della Rete.

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. 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.
Essere consapevoli dell'importanza strategica della protezione cibernetica delle infrastrutture critiche. Comprendere l'importanza fondamentale della sicurezza informatica e della protezione dei dati immateriali. 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). Le diverse figure del Responsabile della conservazione digitale e del Responsabile del servizio di conservazione digitale,
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, comprenderne rischi e vantaggi.
Il Regolamento UE 910/2014 ed il D. Lgs. 179/2016. Considerazioni sulle novità apportate e le profonde conseguenze operative sulla gestione dei flussi documentali dematerializzati.

Opportunità e rischi della Rete: Introduzione ad Open data, deep web, criptovalute,