

Diritto e ICT

Modulo 4 – Gestione documentale e dematerializzazione (Versione 1.0)

Il seguente Syllabus riguarda il Modulo 4 *Gestione documentale e dematerializzazione* ed è finalizzato alla conoscenza pratica degli aspetti operativi inerenti alla gestione documentale, alla dematerializzazione, classificazione, organizzazione, assegnazione, reperimento e conservazione amministrativo-giuridica dei documenti informatici acquisiti dalle amministrazioni.

Sezione	Tema	Rif.	Argomento
4.1 Identità Digitali	4.1.1 La carta nazionale dei servizi	4.1.1.1	Conoscere la Carta Nazionale dei Servizi (CNS) e saper descrivere le sue specifiche tecniche.
		4.1.1.2	Sapere che la corrispondenza informatica tra CNS e CIE (Carta d'Identità Elettronica) assicura l'interoperabilità tra le due carte..
		4.1.1.3	Saper raggiungere e consultare l'elenco pubblico dei certificatori che emettono certificati CNS attraverso l'AgID.
	4.1.2 Le firme elettroniche	4.1.2.1	Definire, secondo il disposto normativo vigente, la firma elettronica.
		4.1.2.2	Definire, secondo il disposto normativo vigente, la firma grafometrica e fornire le principali caratteristiche.
		4.1.2.3	Conoscere le caratteristiche della firma digitale.
		4.1.2.4	Comprendere che la firma digitale è il risultato di una procedura informatica, detta validazione, che garantisce l'autenticità, l'integrità e il non ripudio di documenti informatici.
		4.1.2.5	Definire la differenza intercorrente tra firma elettronica qualificata e firma digitale, in riferimento all'algoritmo di crittografia a doppia chiave asimmetrica, utilizzato dalla firma digitale.
		4.1.2.6	Descrivere le differenze, tra le varie tipologie di firma elettronica, in riferimento alla validità ai fini legali e probatori.
		4.1.2.7	Conoscere i compiti che l'AgID svolge in riferimento ai certificatori accreditati.
4.1.2.8	Illustrare che i certificatori accreditati forniscono servizi di certificazione ed emettono certificati qualificati (per la firma digitale) e certificati di autenticazione (per le carte nazionali dei servizi) per conto delle pubbliche amministrazioni.		



Sezione	Tema	Rif.	Argomento
		4.1.2.9	Conoscere la procedura per richiedere la firma digitale, anche avvalendosi della tabella dei certificatori riportata sul sito dell'AgID.
		4.1.2.10	Conoscere le implicazioni che i certificati digitali revocati, scaduti o sospesi determinano sulla validità legale dei documenti informatici sottoscritti con firma elettronica qualificata o digitale.
		4.1.2.11	Definire, secondo il disposto normativo vigente, i formati di firma consentiti (CAAdES, PAdES e XAdES)
		4.1.2.12	Essere in grado di configurare Acrobat (Professional e Reader) per verificare la firma digitale nel formato PAdES.
		4.1.2.13	Saper generare una firma digitale tramite la crittografia a doppia chiave o nel formato PDF attualmente in uso.
		4.1.2.14	Saper effettuare la verifica della firma digitale e la successiva estrazione degli oggetti firmati tramite applicazioni messe a disposizione da pubblici gestori o utilizzando l'applicazione europea Digital Signature Service (DSS), in modo conforme al disposto normativo vigente.
		4.1.2.15	Saper mantenere sempre aggiornati i prodotti di firma e verifica delle firme digitali in uso.
	4.1.3 La marca temporale	4.1.3.1	Definire, secondo il disposto normativo vigente, la marca temporale.
		4.1.3.2	Comprendere la differenza tra marca temporale e riferimento temporale.
		4.1.3.3	Definire il ruolo delle Time Stamping Authority (TSA).
		4.1.3.4	Sapere che il servizio di marcatura temporale si basa sull'uso delle funzioni di hashing.
		4.1.3.5	Comprendere la necessità di attestare una data certa sul documento informatico attraverso il servizio di marca temporale (timestamping) e definire fasi e peculiarità.
		4.1.3.6	Comprendere l'utilità della marca temporale nel caso di documenti su cui sia stata apposta una firma digitale..
		4.1.3.7	Conoscere la modalità di utilizzo delle due differenti tipologie di formato: m7m (attached) e tsr (detached).

- 4.1.3.8 Saper marcare temporalmente un documento informatico..
- 4.1.4 I Sistemi per l'identificazione a distanza
- 4.1.4.1 Comprendere come i sistemi d'identità federata evitano la gestione centralizzata delle credenziali e delle informazioni personali, consentendo agli utenti di collegare la propria identità tra i vari account distribuiti.
- 4.1.4.2 Conoscere le iniziative di e-Government in tema d'identità federata e d'identificazione a distanza, come il Sistema Pubblico di Connettività e Cooperazione (SPC) e il Progetto ICAR.
- 4.1.4.3 Definire il Servizio di Interoperabilità, Cooperazione ed Accesso (SICA), come una infrastruttura, non riconducibile a nessuna amministrazione specifica, in grado di supportare e facilitare la cooperazione fra amministrazioni.
- 4.1.4.4 Descrivere i sistemi d'identità federata, in termini di Identity Management e Role Based Access Control (RBAC) e Identity Provider.
- 4.1.4.5 Definire gli elementi fondamentali del modello di identità federata (identità, autenticazione, attributo, profilo utente, ruolo, profilo del servizio).
- 4.1.4.6 Comprendere e definire il Sistema Pubblico per la gestione dell'Identità Digitale (SPID) come un valido strumento, per il cittadino, per l'accesso ai servizi in rete della PA.
- 4.1.4.7 Definire Italia Login come il nuovo portale di autenticazione della pubblica amministrazione.
- 4.1.4.8 Conoscere le tecniche utilizzate dalle smartcard con doppio microprocessore, a radiofrequenza e a contatti.
- 4.1.4.9 Sapere che un documento digitale unico (DDU) sostituirà la carta d'identità e la tessera sanitaria e offrirà al cittadino la possibilità di accedere in via telematica ai servizi erogati dalle amministrazioni pubbliche.
- 4.1.4.10 Descrivere le interrelazioni tra SPID, carta d'identità elettronica, carta nazionale dei servizi e regolamento europeo eIDAS.
- 4.1.4.11 Comprendere che il SPID realizza un modello federato nel quale oltre alle identità personali sono gestiti i ruoli, i titoli e le qualifiche professionali.



Sezione	Tema	Rif.	Argomento	
4.2 Documento Informatico	4.2.1 Formazione e gestione dei documenti informatici	4.1.4.12	Saper descrivere la differenza tra i certificati di attributo PKC e gli Attribute Certificate (AC).	
		4.2.1.1	Comprendere che il documento informatico è definito come “la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti” ed è elemento indispensabile per la dematerializzazione dell’azione amministrativa.	
		4.2.1.2	Sapere che le pubbliche amministrazioni formano gli originali dei propri documenti con mezzi informatici, secondo il disposto normativo vigente.	
		4.2.1.3	Definire le procedure di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici, in riferimento alle regole tecniche vigenti.	
	4.2.2 Immodificabilità dei documenti informatici	4.2.1.4	Determinare le varie modalità con le quali è formato un documento informatico, secondo le regole tecniche vigenti.	
		4.2.2.1	Definire il concetto di immodificabilità del documento informatico e saper determinare le varie modalità con le quali un documento informatico è reso immodificabile.	
	4.2.3 Duplicati, copie ed estratti di documenti informatici e analogici	4.2.2.2	Definire il concetto di impronta di un documento informatico e le procedure per saperla calcolare.	
		4.2.3.1	Definire le modalità, previste dal disposto normativo vigente, riferite alla copia informatica o per immagine su supporto informatico di un documento analogico.	
		4.2.3.2	Descrivere sotto quali condizioni le copie informatiche di documenti analogici o copie analogiche di documenti informatici, hanno la stessa validità legale.	
		4.2.3.3	Conoscere le linee guida AgID per le modalità tecniche di generazione, apposizione e verifica del contrassegno generato elettronicamente.	
			4.2.3.4	Descrivere il processo di generazione, apposizione e verifica e saper generare, apporre e verificare un contrassegno generato elettronicamente.

Sezione	Tema	Rif.	Argomento
	4.2.4 Linee guida per il contrassegno generato elettronicamente (Il Timbro Digitale o Glifo)	4.2.4.1	Descrivere come l'apposizione del contrassegno a stampa (Timbro Digitale o Glifo) consenta la verifica della conformità del documento analogico, rispetto all'originale informatico.
		4.2.4.2	Comprendere come il contrassegno generato elettronicamente (Timbro Digitale o Glifo) corrisponde a una sequenza di bit codificata e idonea a rappresentare un documento amministrativo informatico, un suo estratto, una sua copia, un suo duplicato o i suoi dati identificativi.
		4.2.4.3	Conoscere le linee guida AgID per le modalità tecniche di generazione, apposizione e verifica del contrassegno generato elettronicamente.
		4.2.4.4	Descrivere il processo di generazione, apposizione e verifica e saper generare, apporre e verificare un contrassegno generato elettronicamente.
		4.2.4.5	Individuare le idonee misure atte a consentire un corretto trattamento per la protezione dei dati personali, durante la generazione del contrassegno generato elettronicamente.
	4.2.5 Il documento amministrativo informatico.	4.2.5.1	Descrivere le indicazioni specifiche per i documenti amministrativi informatici, previste dalla regole tecniche vigenti, in tema di formazione, identificazione e gestione, immutabilità e integrità.
		4.2.5.2	Descrivere le indicazioni specifiche relative ai documenti amministrativi informatici, in tema di fascicoli, registri e repertori informatici..
	4.2.6 Il fascicolo informatico	4.2.6.1	Sapere che il fascicolo informatico è realizzato garantendo la possibilità di essere direttamente consultato ed alimentato da tutte le amministrazioni coinvolte nel procedimento.
		4.2.6.2	Conoscere le parti costituenti Il fascicolo informatico, in modo da garantire corretta collocazione, facile reperibilità e collegabilità, in relazione al contenuto ed alle finalità, dei singoli documenti.
		4.2.6.3	Saper utilizzare un sistema per produrre un fascicolo elettronico documentale.

Sezione	Tema	Rif.	Argomento
	4.2.7 Riproduzione e conservazione dei documenti.	4.2.7.1	Essere a conoscenza dell'obbligo che le PA hanno di valutare il recupero su supporto informatico dei documenti e degli atti cartacei dei quali sia obbligatoria o opportuna la conservazione.
		4.2.7.2	Sapere che per mantenerne validità e rilevanza a tutti gli effetti di legge, la riproduzione e la conservazione nel tempo di atti, dati e documenti devono essere effettuate in modo da garantire la conformità dei documenti agli originali.
		4.2.7.3	Sapere che i documenti informatici, di cui è prescritta la conservazione per legge o regolamento, possono essere archiviati per le esigenze correnti anche con modalità cartacee e sono conservati in modo permanente con modalità digitali.
	4.2.8 I metadati	4.2.8.1	Conoscere il ruolo dei metadati nel processo di autenticazione, ricerca, localizzazione del documento informatico e saper definire le varie tipologie.
		4.2.8.2	Descrivere l'insieme minimo dei metadati, così come previsto dalla regole tecniche vigenti.
	2.2.9 I documenti originali non unici	4.2.9.1	Definire i documenti originali analogici unici e non unici, delineando i criteri che indicano le modalità di conservazione.
		4.2.9.2	Sapere che il disposto normativo vigente ha eliminato, per tutti i documenti analogici originali unici, l'impedimento alla dematerializzazione dei documenti connotati da uno scarso rilievo pubblicistico.
	4.2.10 I flussi documentali in forma digitale	4.2.10.1	Conoscere le modalità con cui è sviluppato il processo di digitalizzazione dei procedimenti amministrativi.
		4.2.10.2	Utilizzare strumenti e tecniche di conservazione, supportando l'archiviazione dei documenti informatici e delle copie.
		4.2.10.3	Definire e comprendere la differenza tra la gestione informatica dei documenti e il sottosistema per la gestione informatica dei documenti.
		4.2.10.4	Descrivere i requisiti del sottosistema di gestione informatica dei documenti.

Sezione	Tema	Rif.	Argomento
		4.2.10.5	Comprendere come la gestione documentale garantisce la validità legale dei documenti informatici basandosi sul sistema stesso invece che sugli strumenti classici (firma digitale, marca temporale, timbro digitale, PEC).
		4.2.10.6	Comprendere come la gestione dei flussi documentali organizza e governa la documentazione ricevuta, inviata o comunque prodotta dall'amministrazione.
		4.2.10.7	Descrivere il ciclo di vita dei documenti nella gestione documentale (produzione, gestione e conservazione).
		4.2.10.8	Descrivere la fase di produzione della gestione documentale e i suoi sottoprocessi fondamentali (creazione e acquisizione).
		4.2.10.9	Descrivere la fase di gestione della gestione documentale e i suoi sottoprocessi fondamentali (utilizzo e trasmissione).
		4.2.10.10	Descrivere la fase di conservazione della gestione documentale e i suoi sottoprocessi fondamentali.
	4.2.11 Il Protocollo informatico	4.2.11.1	Definire il titolario di classificazione come lo strumento dell'archivio corrente che serve per dividere la documentazione prodotta o ricevuta da un soggetto in settori e categorie.
		4.2.11.2	Definire le tre funzionalità base previste per il protocollo informatico (il nucleo minimo).
		4.2.11.3	Saper indicare la tipologia di informazioni minime e accessorie associate ai messaggi scambiati tra le pubbliche amministrazioni.
		4.2.11.4	Saper indicare in che modo viene garantita l'interoperabilità delle signature tra i vari sistemi di protocollo informatico.
		4.2.11.5	Conoscere le regole tecniche vigenti per il protocollo informatico.
		4.2.11.6	Indicare i criteri che descrivono il sistema di gestione, anche ai fini della conservazione, dei documenti informatici e fornisce le istruzioni per la corretta gestione dei flussi documentali e degli archivi.
		4.2.11.7	Sapere che è obbligatoria la stesura e la pubblicazione sul sito internet del manuale di gestione del protocollo informatico dei flussi documentali e degli archivi.

Sezione	Tema	Rif.	Argomento
		4.2.11.8	Indicare le informazioni minime da includere nella segnatura di protocollo in entrata e in uscita.
		4.2.11.9	Saper utilizzare un sistema per la protocollazione dei documenti in entrata e in uscita.
		4.2.11.10	Sapere che, secondo le regole tecniche vigenti, l'invio in conservazione del registro di protocollo informatico deve essere eseguita entro la giornata lavorativa successiva, garantendone l'immodificabilità del contenuto.
	4.2.12 La Trasmissione informatica dei documenti	4.2.12.1	Spiegare il significato di valore giuridico della trasmissione dei documenti trasmessi da chiunque ad una PA, secondo il disposto normativo vigente..
		4.2.12.2	Determinare la validità, ai fini del procedimento amministrativo, della trasmissione dei documenti attraverso la posta elettronica tra le pubbliche amministrazioni.
		4.2.12.3	Determinare i casi in cui le comunicazioni sono valide, ai fini della verifica della provenienza..
		4.2.12.4	Specificare che le pubbliche amministrazioni provvedono ad istituire e pubblicare nell'Indice PA almeno una casella di posta elettronica certificata per ciascun registro di protocollo..
		4.2.12.5	Specificare che le pubbliche amministrazioni utilizzano per le comunicazioni tra l'amministrazione ed i propri dipendenti la posta elettronica o altri strumenti informatici di comunicazione.
		4.2.12.6	Determinare le caratteristiche principali della posta elettronica certificata (PEC).
		4.2.12.7	Definire la Posta Elettronica Certificata (PEC) in base al disposto normativo vigente, con particolare riferimento alla validità giuridica, al concetto di Busta Elettronica, al significato di ricevuta elettronica di invio/ritorno e alla certezza della provenienza e destinazione.
		4.2.12.8	Definire le garanzie, ai fini legali e probatori, che il servizio di posta elettronica certificata determina.
		4.2.12.9	Comprendere che le condizioni sotto le quali data e ora di trasmissione e di ricezione di un documento informatico, sono opponibili ai terzi.

Sezione	Tema	Rif.	Argomento
		4.2.12.10	Conoscere le garanzie di sicurezza, a livello fisico e informatico, che i sistemi di PEC forniscono.
		4.2.12.11	Saper utilizzare un sistema di PEC per spedire una e-mail certificata e verificare l'avvenuta consegna e ricezione della stessa.
		4.2.12.12	Conoscere le implicazioni riguardanti l'invio di PEC ad un utente con casella PEC, ad un utente privo di PEC e viceversa.
4.3 Dematerializzazione dei documenti e degli atti cartacei della PA.	4.3.1 La dematerializzazione dei documenti nella PA.	4.3.1.1	Sapere che le pubbliche amministrazioni valutano in termini di rapporto tra costi e benefici il recupero su supporto informatico dei documenti e degli atti cartacei dei quali sia obbligatoria o opportuna la conservazione, in base al disposto normativo vigente.
		4.3.1.2	Sapere che le pubbliche amministrazioni provvedono alla predisposizione dei conseguenti piani di sostituzione degli archivi cartacei con archivi informatici, nel rispetto delle regole tecniche.
		4.3.1.3	Conoscere che il DPCM del 3 dicembre 2013 sulle regole tecniche in materia di conservazione digitale, hanno sostituito integralmente le disposizioni della Delibera CNIPA n. 11/2004 del 19 febbraio 2004.
		4.3.1.4	Sapere che il DPCM del 13 novembre 2014 sulle regole tecniche in materia di documenti informatici individua le caratteristiche e le procedure di formazione e chiusura del documento informatico.
		4.3.1.5	Conoscere che la chiusura di documento informatico avviene attraverso l'utilizzo di processi o strumenti informatici al fine di renderlo immutabile durante le fasi della gestione documentale di tenuta, accesso e conservazione.
		4.3.1.6	Determinare le diverse modalità per rendere immutabile un documento informatico, attraverso le procedure dei sistemi di gestione documentale.
	4.3.2 I sistemi per la conservazione digitale	4.3.2.1	Definire il sistema di conservazione digitale e i suoi principali riferimenti normativi..

Sezione	Tema	Rif.	Argomento
		4.3.2.2	Descrivere come Il sistema di conservazione mira a garantire le caratteristiche di autenticità, integrità, affidabilità, leggibilità e reperibilità dei documenti e dei fascicoli informatici, come previsto dal disposto normativo vigente.
		4.3.2.3	Conoscere che è obbligatorio predisporre idonee misure per la qualità e la sicurezza fisica, logica e tecnologica dei sistemi, consentendo l'accesso controllato a dati, documenti e informazioni.
		4.3.2.4	Conoscere che le regole tecniche descrivono i modelli organizzativi dei sistemi di conservazione digitale, individuando ruoli e responsabilità specifiche.
		4.3.2.5	Conoscere che le regole tecniche individuano le figure del produttore dei documenti, dell'utente e del responsabile della conservazione.
		4.3.2.6	Definire il ruolo del produttore e dell'utente del sistema di conservazione digitale, ai sensi delle regole tecniche vigenti.
		4.3.2.7	Definire il ruolo e i compiti del responsabile del sistema di conservazione, ai sensi delle regole tecniche vigenti.
		4.3.2.8	Saper che le regole tecniche impongono la produzione del manuale della conservazione in cui sono descritti: l'organizzazione, i soggetti coinvolti e i ruoli degli stessi, l'architettura e l'infrastruttura utilizzata, il sistema di sicurezza, il processo della conservazione, le modalità di esibizione e i formati degli oggetti destinati alla conservazione.
		4.3.2.9	Conoscere gli allegati alle regole tecniche vigenti.
		4.3.2.10	Sapere che il processo di conservazione digitale determina efficienza gestionale e riduzione di tempi e costi.
		4.3.2.11	Definire i pacchetti informativi come oggetti fondamentali della conservazione digitale, elencando le diverse tipologie: versamento, archiviazione, distribuzione.
		4.3.2.12	Descrivere la funzione dei pacchetti informativi di versamento, archiviazione e distribuzione.
		4.3.2.13	Definire le fasi del processo di conservazione.

Sezione	Tema	Rif.	Argomento
		4.3.2.14	Conoscere le problematiche complesse della conservazione digitale nel lungo periodo, riferite ai requisiti tecnologici, organizzativi e archivistici.
		4.3.2.15	Sapere che sono fatti salvi i poteri di controllo del Ministero per i beni e le attività culturali sugli archivi delle amministrazioni pubbliche e sugli archivi privati dichiarati di notevole interesse storico.
		4.3.2.16	Definire le condizioni sotto le quali, nella pubblica amministrazione, è possibile delegare il ruolo di responsabile della conservazione digitale e di responsabile della gestione documentale.
	4.3.3 I formati per la conservazione digitale	4.3.3.1	Definire in cosa consiste il formato della conservazione digitale, in termini di leggibilità, interpretazione e capacità di elaborazione.
		4.3.3.2	Conoscere le varie caratteristiche dei formati per la conservazione digitale, ai fini della scelta.
		4.3.3.3	Definire il grado di sicurezza e la portabilità di un formato per la conservazione digitale.
		4.3.3.4	Definire funzionalità, supporto allo sviluppo e diffusione di un formato per la conservazione digitale.
		4.3.3.5	Conoscere i formati più comuni per la conservazione digitale e il PDF/A.