Diritto e ICT
Modulo 1 – Protezione Dati Personali – Privacy e Sicurezza (Versione 1.0)

Il seguente Syllabus riguarda il Modulo 1, *Protezione dei dati personali*, ed è finalizzato alla conoscenza dei princìpi della protezione dei dati personali nella normativa europea e italiana.

Scopi del modulo

Modulo 1 Questo modulo è indirizzato a giuristi, avvocati, magistrati, notai, commercialisti, ingegneri, dipendenti degli studi professionali, responsabili dei sistemi informativi, tecnici informatici e consulenti informatici, dirigenti scolastici, insegnanti e formatori, responsabili di laboratori, funzionari e dipendenti della PA e degli Enti Locali, personale appartenente alle forze dell'ordine, responsabili della privacy.

Il modulo – Protezione Dati Personali richiede che il Candidato conosca l'evoluzione del concetto di privacy e la normativa italiana sulla privacy, i contenuti del Codice in materia di protezione dei dati personali, la figura dell'autorità Garante e il Gruppo dei Garanti europei. Il Candidato deve comprendere le norme generali che regolano il trattamento dei dati personali e le particolarità di alcuni settori specifici di trattamento. Il Candidato deve essere consapevole degli obblighi di sicurezza richiesti, della redazione del Documento Programmatico sulla Sicurezza e delle responsabilità e sanzioni previste dal Codice. Il Candidato deve conoscere le norme in materia di comunicazioni elettroniche non sollecitate e alcune particolari fattispecie di trattamenti illeciti.

Sezione	*Tema*	*Rif.*	*Argomento*
1.1 Protezione dei dati personali e sicurezza	1.1.1 Evoluzione della Privacy	1.1.1.1	Conoscere l'origine del diritto alla privacy, l'origine del concetto: "the right to privacy"; (dalla nascita alla Direttiva Europea 95/46/CE).
		1.1.1.2	Comprendere le principali linee guida e interventi legislativi internazionali, il ruolo dell'O.C.S.E. e del Consiglio d'Europa, la Convenzione di Strasburgo.
		1.1.1.3	Conoscere l'evoluzione del diritto alla privacy in Italia.
	1.1.2 La Normativa nazionale sulla Privacy	1.1.2.1	Conoscere il c.d. "Codice della privacy": aspetti generali e struttura del Codice.
		1.1.2.2	Sapere quali sono i principi fondamentali (finalità, necessità, liceità, correttezza, proporzionalità, completezza, non eccedenza).
		1.1.2.3	Conoscere le principali definizioni.
		1.1.2.4	Comprendere le tipologie di dati (personali, sensibili, "quasi" sensibili, giudiziari, anonimi).
		1.1.2.5	Identificare e riconoscere i ruoli delle figure previste (interessato, titolare, responsabile, incaricato), redigere e valutare le nomine.

AICA
Associazione Italiana per l'Informatica ed il Calcolo Automatico

Sezione	Tema	Rif.	Argomento
		1.1.2.6	Conoscere e valutare l'informativa (definizione, funzione, contenuti minimi obbligatori, le regole di rilascio, i casi particolari).
		1.1.2.7	Comprendere il significato della comunicazione e diffusione dei dati.
		1.1.2.8	Conoscere il consenso (funzione, contenuti e forma, il consenso nel trattamento dei dati sensibili, il rapporto tra consenso e informativa, i casi di esclusione).
		1.1.2.9	Essere consapevoli del diritto alla protezione dei dati personali e dei diritti degli interessati.
	1.1.3 L'Autorità garante per la tutela dei dati personali	1.1.3.1	Conoscere funzioni del Garante della privacy, segnalazioni, reclami e ricorsi, controlli, provvedimenti, notifica al Garante.
		1.1.3.2	Conoscere lo scopo del gruppo dei Garanti europei.
	1.1.4 Specifici settori di trattamento	1.1.4.1	Comprendere il trattamento dei soggetti pubblici e le finalità di rilevante interesse pubblico; il trattamento in anagrafi ed elettorale; scopi storici e scientifici.
		1.1.4.2	Conoscere il trattamento in ambito sanitario.
		1.1.4.3	Conoscere il trattamento in ambito giudiziario e nelle forze di polizia e di sicurezza.
		1.1.4.4	Essere consapevoli degli aspetti del trattamento delle informazioni nella scuola e istruzione; essere consapevoli delle implicazioni e delle responsabilità per quanto riguarda i minori e gli studenti.
		1.1.4.5	Sapere le disposizioni sul trasferimento dei dati all'estero.
	1.1.5 La Sicurezza delle Informazioni	1.1.5.1	Comprendere gli obblighi di sicurezza, la sicurezza e lo sviluppo tecnologico, l'obiettivo di minimizzare i rischi.
		1.1.5.2	Conoscere e valutare le misure minime di sicurezza per i trattamenti con l'ausilio di strumenti elettronici.
		1.1.5.3	Comprendere l'autenticazione informatica, le credenziali di autenticazione e le procedure di gestione.

Sezione	Tema	Rif.	Argomento
		1.1.5.4	Saper definire il sistema di autorizzazione, l'aggiornamento periodico dell'ambito di trattamento consentito dai singoli incaricati e le classi omogenee di incarico (autorizzazioni).
		1.1.5.5	Descrivere la protezione di dati rispetto ai trattamenti illeciti, accessi non consentiti e l'aggiornamento periodico dei programmi per elaboratore.
		1.1.5.6	Descrivere l'obbligo normativo sulle procedure per le copie di sicurezza (backup) e ripristino della disponibilità dei dati; la corretta gestione dei supporti rimovibili e la cancellazione sicura dei dati.
		1.1.5.7	Identificare i provvedimenti di semplificazione e le istruzioni del garante.
		1.1.5.8	Comprendere l'adozione di cifratura o codici identificativi per determinati trattamenti, idonei a rivelare lo stato di salute o la vita sessuale, effettuati da organismi sanitari.
		1.1.5.9	Conoscere responsabilità e compiti degli amministratori dei sistemi e il relativo provvedimento generale del Garante.
		1.1.5.10	Descrivere le misure minime di sicurezza per i trattamenti senza l'ausilio di strumenti elettronici.
	1.1.6 Il Documento Programmatico sulla Sicurezza (DPS)	1.1.6.1	Definire il documento programmatico sulla sicurezza.
		1.1.6.2	Identificare i contenuti del DPS, i suoi scopi e i tempi per gli adempimenti.
		1.1.6.3	Sapere le modalità di stesura e aggiornamento del DPS e le linee guida del garante.
		1.1.6.4	Essere consapevoli della gestione dei processi organizzativi, delle istruzioni organizzative e delle verifiche.
	1.1.7 Tipologie rilevanti di trattamento	1.1.7.1	Conoscere gli aspetti della privacy nel mondo del lavoro.
		1.1.7.2	Comprendere le disposizioni sulla video-sorveglianza.

Sezione	Tema	Rif.	Argomento
		1.1.7.3	Essere consapevole delle disposizioni sulla privacy e posta elettronica.
		1.1.7.4	Descrivere la privacy su Internet: procedure per informative e consensi su web e in via telematica.
		1.1.7.5	Comprendere le disposizioni riguardanti la privacy digitale: i log e loro conservazione, identificabilità e anonimato (anonimous surfing e remailing, cookies).
		1.1.7.6	Comprendere la sicurezza come processo e conoscere le normative internazionali ISO riguardanti i sistemi di gestione per tutela dell'informazione.
	1.1.8 Responsabilità e Sanzioni	1.1.8.1	Conoscere le differenze tra misure minime e idonee per la sicurezza.
		1.1.8.2	Descrivere le sanzioni previste dal codice della privacy.
		1.1.8.3	Comprendere le disposizioni sui danni cagionati per effetto del trattamento (responsabilità civile e inversione dell'onere della prova).
	1.1.9 Privacy e particolari casi di trattamento illecito	1.1.9.1	Comprendere gli aspetti legati al furto di credenziali (anche attraverso keylogger e virus) e il furto d'identità.
		1.1.9.2	Comprendere gli aspetti legati alla frode informatica e al phishing (le sue fasi e i reati).
		1.1.9.3	Essere consapevoli degli aspetti di tutela della privacy nei social network.
		1.1.9.4	Conoscere la privacy collegata alla diffamazione on line, chat, cyberbullismo, cyber-stalking.
		1.1.9.5	Comprendere gli aspetti legati all'accesso abusivo a sistemi informatici e telematici, danneggiamento informatico e la violazione del domicilio informatico.
1.2 Le comunicazioni non sollecitate	1.2.1 Le comunicazioni elettroniche non sollecitate	1.2.1.1	Saper definire il concetto di spamming.
		1.2.1.2	Conoscere il quadro normativo sulle comunicazioni indesiderate e l'Opt-in, Opt-out.

Sezione	Tema	Rif.	Argomento
		1.2.1.3	Essere consapevole degli aspetti per la prevenzione.
		1.2.1.4	Identificare o riconoscere le responsabilità e le sanzioni, i provvedimenti e le indicazioni del Garante.
		1.2.1.5	Comprendere le disposizioni in materia di telemarketing.
	1.2.2 Le Comunicazioni Telefoniche o con altri mezzi	1.2.2.1	Conoscere la riservatezza e il quadro normativo sulle comunicazioni indesiderate.

Diritto e ICT
Modulo 2 – Firma Digitale e Posta Elettronica Certificata (Versione 1.0)

Il seguente Syllabus riguarda il Modulo 2 *Firma Digitale e Posta Elettronica Certificata* ed è finalizzato alla conoscenza pratica degli aspetti operativi inerenti la Posta Elettronica Certificata e la Firma Digitale.

Scopi del modulo

Modulo 2 Questo modulo è indirizzato a giuristi, avvocati, magistrati, notai, commercialisti, ingegneri, dipendenti degli studi professionali, responsabili dei sistemi informativi, tecnici informatici e consulenti informatici, dirigenti scolastici, insegnanti e formatori, responsabili di laboratori, funzionari e dipendenti della PA e degli Enti Locali, personale appartenente alle forze dell'ordine, responsabili della privacy.

Il modulo – Firma Digitale e Posta Elettronica Certificata richiede che il Candidato conosca le caratteristiche legali della Firma Digitale, il suo funzionamento, i certificati ed il ruolo degli enti certificatori, il suo utilizzo pratico ed il software di firma. Inoltre che il Candidato conosca le caratteristiche legali della Posta Elettronica Certificata, il suo funzionamento, i protocolli di comunicazione utilizzati, le sue caratteristiche di sicurezza ed affidabilità ed il suo utilizzo pratico.

Sezione	*Tema*	*Rif.*	*Argomento*
2.1. Posta Elettronica Certificata	2.1.1 La Posta Elettronica	2.1.1.1	Comprendere i vantaggi della posta elettronica, quali: rapidità di consegna, economicità, possibilità di usare la posta elettronica in luoghi diversi attraverso account basati su siti web.
		2.1.1.2	Capire come è composto un indirizzo di posta elettronica.
		2.1.1.3	Comprendere l'importanza della netiquette (galateo della rete): descrizione accurata dell'oggetto dei messaggi di posta elettronica, concisione nelle risposte, controllo ortografico della posta in uscita.
		2.1.1.4	Conoscere i fondamenti del funzionamento dei protocolli POP3, SMTP, IMAP.
	2.1.2 Considerazioni sulla sicurezza	2.1.2.1	Conoscere i limiti della posta elettronica (trasmissione in chiaro, spedizione senza password, …).
		2.1.2.2	Conoscere le minacce alla sicurezza provenienti da siti web, quali: virus, worm, cavalli di Troia, spyware, phishing. Comprendere il termine "malware".
		2.1.2.3	Conoscere il pericolo di infettare il computer con virus aprendo messaggi sconosciuti o allegati presenti nei messaggi.

AICA
Associazione Italiana per l'Informatica ed il Calcolo Automatico

Sezione	Tema	Rif.	Argomento
	2.1.3 La Posta Elettronica Certificata (PEC)	2.1.3.1	Sapere cosa è la Posta Elettronica Certificata.
		2.1.3.2	Conoscere i principali vantaggi della Posta Elettronica Certificata rispetto ad altri canali di comunicazione.
		2.1.3.3	Conoscere gli ambiti di applicazione del servizio di PEC (Pubblica Amministrazione, Aziende, Privati).
		2.1.3.4	Le comunicazioni con la Pubblica Amministrazione.
		2.1.3.5	Aspetti legali e normative di riferimento.
	2.1.4 Caratteristiche della Posta Elettronica Certificata (PEC)	2.1.4.1	Sapere cosa sono punto di accesso, punto di destinazione, busta di trasporto, punto di ricezione, punto di consegna.
		2.1.4.2	Conoscere le possibilità di interoperabilità (messaggi di posta tra domini di posta certificata e non).
		2.1.4.3	Sapere come funziona la ricevuta elettronica di invio/ritorno: dalla presa in carico all'avvenuta consegna.
		2.1.4.4	Smarrimento della ricevuta elettronica e della posta elettronica certificata.
		2.1.4.5	Saper distinguere tra messaggi firmati e cifrati.
		2.1.4.6	Saper riconoscere la provenienza e destinazione di un messaggio PEC: certezza del mittente, certificazione dell'invio, della consegna e del ricevimento (data e ora).
		2.1.4.7	Conoscere l'importanza di garantire la certezza del contenuto e la sua non modificabilità.
	2.1.5 Utilizzi della Posta Elettronica Certificata (PEC)	2.1.5.1	Sapere come richiedere e attivare una casella di Posta Elettronica Certificata (PEC).
		2.1.5.2	Sapere a chi richiedere una casella di Posta Elettronica Certificata (PEC).
		2.1.5.3	Sapere identificare un messaggio di PEC.
		2.1.5.4	Inviare un messaggio di PEC a un utente con casella PEC.

Sezione	Tema	Rif.	Argomento
		2.1.5.5	Inviare un messaggio di PEC a un utente privo di PEC e viceversa.
		2.1.5.6	Sapere come si verifica un messaggio di PEC (mittente e destinatario).
		2.1.5.7	Sapere come si verificano le ricevute di invio/ritorno.
		2.1.5.8	Sapere come si verifica la Firma Digitale contenuta in un messaggio di PEC.
2.2 Firma Digitale	2.2.1 La Firma Digitale	2.2.1.1	Sapere cosa è una Firma Digitale.
		2.2.1.2	Sapere cosa è il certificato digitale (formato, rilascio e informazioni contenute).
		2.2.1.3	Normative di riferimento, italiane e europee.
	2.2.2 Caratteristiche della Firma Digitale	2.2.2.1	Comprendere il termine “crittografia”.
		2.2.2.2	Conoscere le proprietà dei sistemi a chiave simmetrica e a chiavi asimmetriche (pubbliche e private).
		2.2.2.3	Principi di integrità, autenticazione e non ripudio.
		2.2.2.4	Conoscere il ruolo degli enti certificatori.
		2.2.2.5	Firma elettronica e firma elettronica qualificata, la firma digitale: definizioni e diversa validità giuridica.
		2.2.2.6	Sapere cosa è un certificato digitale associato a un sito web.
	2.2.3 Utilizzi della Firma Digitale	2.2.3.1	Conoscere lo schema di funzionamento della Firma Digitale.
		2.2.3.2	Saper riconoscere i formati dei file firmati.
		2.2.3.3	Conoscere e utilizzare i supporti informatici, hardware e software, per la Firma Digitale.
		2.2.3.4	Conoscere l'importanza della verifica della data certa di un documento informatico.
		2.2.3.5	Conoscere le modalità di apposizione della Firma Digitale.
		2.2.3.6	Conoscere le norme di validità e controllo della Firma Digitale e del certificato digitale.

Sezione	Tema	Rif.	Argomento
		2.2.3.7	Conoscere gli utilizzi comuni di un documento digitale firmato.

Diritto e ICT
Modulo 3 – E-Governance e Amministrazione Digitale (Versione 1.0)

Il seguente Syllabus riguarda il Modulo 3 *E-Governance e Amministrazione Digitale* ed è finalizzato alla conoscenza pratica degli aspetti operativi inerenti alla normativa alla base dell'e-government in Italia e i procedimenti interessati dall'Amministrazione Digitale

Sezione	*Tema*	*Rif.*	*Argomento*
3.1 E-governance in Italia e in Europa	3.1.1 La Strategia EU2020	3.1.1.1	Descrivere la strategia Europa 2020, con riferimento ai cinque obiettivi quantitativi.
		3.1.1.2	Conoscere le sette iniziative prioritarie di Europa 2020.
	3.1.2 EU e-Government Action Plan	3.1.2.1	Descrivere le linee di azione del piano comunitario.
		3.1.2.2	Descrivere gli interventi prefigurati per ciascuna delle linee di intervento
	3.1.3 L'Agenda Digitale Italiana	3.1.3.1	Saper indicare i riferimenti normativi dell'Agenda Digitale Italiana.
		3.1.3.2	Saper indicare i riferimenti normativi dell'Agenda Digitale Italiana.
		3.1.3.3	Saper definire l'interoperabilità tra i sistemi informativi della PA.
		3.1.3.4	Descrivere Il Piano strategico banda ultralarga
		3.1.3.5	Conoscere il significato di Open Data.
		3.1.3.6	Conoscere ed elencare le competenze di base: competenze di e-leadership, competenze specialistiche, competenze sviluppate dal piano nazionale scuola digitale.
		3.1.3.7	Descrivere il significato e le caratteristiche delle Città e Comunità intelligenti (Smart City).
		3.1.3.8	Definire le responsabilità dell'AgID, in riferimento alla Smart City.
		3.1.3.9	Definire il ruolo e i compiti dell'AgID in riferimento ai Progetti Europei e Internazionali.
	3.1.4 Il Codice dell'Amministrazione Digitale	3.1.4.1	Conoscere il riferimento normativo al Nuovo Codice dell'Amministrazione Digitale.
		3.1.4.2	Illustrare i due principi sui quali si basa il nuovo Codice dell'Amministrazione Digitale.
		3.1.4.3	Conoscere i DPCM che individuano le regole tecniche che integrano il Nuovo Codice dell'Amministrazione Digitale.

AICA
Associazione Italiana per l'Informatica ed il Calcolo Automatico

Sezione	Tema	Rif.	Argomento
		3.1.4.4	Comprendere e descrivere le indicazioni della normativa di riferimento sulla validità dei documenti informatici.
		3.1.4.5	Comprendere e descrivere le indicazioni della normativa di riferimento sulla conservazione digitale dei documenti.
		3.1.4.6	Comprendere e descrivere le indicazioni della normativa di riferimento sulla PEC (Posta Elettronica Certificata).
		3.1.4.7	Comprendere e descrivere le indicazioni della normativa di riferimento riferita a siti pubblici e trasparenza.
		3.1.4.8	Comprendere e descrivere le indicazioni della normativa di riferimento riferita alla customer satisfaction dei cittadini su Internet.
		3.1.4.9	Comprendere e descrivere le indicazioni della normativa di riferimento sull'utilizzo della modulistica della PA on line.
		3.1.4.10	Comprendere e descrivere le indicazioni della normativa di riferimento sulla trasmissione delle informazioni via web.
		3.1.4.11	Comprendere e descrivere le indicazioni della normativa di riferimento per quanto riguarda le comunicazioni tra imprese e amministrazioni.
		3.1.4.12	Comprendere e descrivere le indicazioni della normativa di riferimento sulle firme elettroniche, avanzate, qualificate e digitali.
		3.1.4.13	Comprendere e descrivere le indicazioni della normativa di riferimento per quanto riguarda protocollo informatico, fascicolo elettronico e tracciabilità.
		3.1.4.14	Comprendere e descrivere le indicazioni della normativa di riferimento sulla sicurezza digitale.
	3.1.5 Formazione delle regole sui nomi a dominio in Italia, relative procedure di riassegnazione.	3.1.5.1	Descrivere il ruolo del NIC (Registro.it) come anagrafe dei domini Internet .it.
		3.1.5.2	Individuare ed elencare i compiti del NIC, del DBNA (database dei nomi assegnati) e del DNS (Domain Name System).
		3.1.5.3	Delineare compiti e funzioni del Registro, del Registrar e del Registrante.

Sezione	Tema	Rif.	Argomento
		3.1.5.4	Conoscere l'organizzazione e struttura dei nomi assegnabili nel ccTLD .it.
	3.1.6 I reati commessi su Internet	3.1.6.1	Discriminare tra reati commessi su Internet e reati commessi mediante Internet.
		3.1.6.2	Descrivere i reati commessi su Internet (reati informatici o telematici propri).
		3.1.6.3	Descrivere i reati commessi mediante Internet (reati informatici o telematici impropri).
		3.1.6.4	Definire i reati informatici nell'ordinamento italiano.
		3.1.6.5	Conoscere le norme volte a contrastare l'accesso abusivo ad un sistema informatico o telematico.
		3.1.6.6	Discriminare tra le seguenti categorie di software nocivo: malware, virus, worm, trojan, backdoor, spyware, dialer, hijacker, rootkit, keylogger.
		3.1.6.7	Descrivere e spiegare le norme relative all'intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche.
		3.1.6.8	Descrivere e spiegare le norme relative a Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche.
		3.1.6.9	Descrivere e spiegare le norme relative a falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche.
		3.1.6.10	Definire l'integrità dei sistemi informatici e telematici.
		3.1.6.11	Conoscere la Convenzione di Budapest del Consiglio d'Europa sul Cybercrime approvata il 18 marzo 2008 dal Parlamento italiano.
	3.1.7 Digital copyright e file sharing.	3.1.7.1	Definire l'informazione come bene immateriale: copyright e digital copyright.
		3.1.7.2	Descrivere la responsabilità dell'utente: data retention sul traffico telematico e le sanzioni previste dalla legge sul diritto d'autore.
		3.1.7.3	Definire il digital rights management (la protezione tecnologica).

Sezione	Tema	Rif.	Argomento
3.2 Amministrazione Digitale	3.2.1 La gestione dei procedimenti amministrativi	3.2.1.1	Comprendere cosa si intende per digitalizzazione dei procedimenti amministrativi.
		3.2.1.2	Conoscere i fondamenti della gestione documentale (Document management system)
		3.2.1.3	Descrivere il modello di riferimento del Sistema di Gestione dei Procedimenti Amministrativi della PA (SGPA), definito da AgID.
		3.2.1.4	Saper gestire flussi documentali e protocollo attraverso l'automazione della fase di registrazione dei documenti in ingresso e uscita e relativa assegnazione.
		3.2.1.5	Saper utilizzare tecniche di dematerializzazione attraverso il trattamento dei flussi documentali sia in ingresso che in uscita.
		3.2.1.6	Utilizzare strumenti e tecniche di conservazione, supportando l'archiviazione dei documenti informatici e delle copie.
	3.2.2 La conservazione	3.2.2.1	Definire le caratteristiche del sistema di conservazione digitale.
		3.2.2.2	Descrivere le modalità operative per realizzare l'attività di conservazione.
		3.2.2.3	Conoscere le modalità di accreditamento dei conservatori e saper consultare l'elenco dei conservatori accreditati
	3.2.3 I pagamenti e la fatturazione elettronica	3.2.3.1	Conoscere PagoPA, il sistema dei Pagamenti elettronici a favore delle PA e dei gestori dei servizi di pubblica utilità.
		3.2.3.2	Utilizzare un software per la generazione delle fatture elettroniche.
		3.2.3.3	Descrivere e spiegare il significato del Codice IPA, CIG e CUP.
		3.2.3.4	Utilizzare gli strumenti, disponibili sul sito FatturaPA, utili per facilitare il processo di fatturazione elettronica.
	3.2.4 La registrazione al dominio .gov.it	3.2.4.1	Conoscere la Direttiva del Ministro per la PA che fissa i criteri di riconoscibilità, di aggiornamento, di usabilità e accessibilità dei siti della PA, individuando con il gov.it, il dominio che riconosce i siti e i portali delle stesse.

Sezione	Tema	Rif.	Argomento
		3.2.4.2	Descrivere la procedura per la registrazione al dominio gov.it.
	3.2.5 Trasparenza Amministrativa e Siti Web della PA	3.2.5.1	Definire i caratteri dell'Amministrazione Trasparente e il diritto di accesso civico, in relazione alla normativa privacy e alle responsabilità derivanti dell'inclusione dei social network.
		3.2.5.2	Conoscere le principali caratteristiche dell'Albo online (pubblicità legale).
		3.2.5.3	Saper utilizzare l'Albo online (pubblicità legale).
		3.2.5.4	Definire le modalità di pubblicazione degli atti e le responsabilità derivanti.
	3.2.6 Accessibilità e Usabilità	3.2.6.1	Definire il requisito di accessibilità di un sito web.
		3.2.6.2	Definire il requisito di usabilità di un sito web e saper elencare i vantaggi derivanti.
	3.2.7 Sanità digitale	3.2.7.1	Conoscere il termine sanità digitale.
		3.2.7.2	Comprendere le modalità d'impiego del Fascicolo Sanitario Elettronico (FSE).
		3.2.7.3	Conoscere le modalità d'uso della Tessera sanitaria (TS) valida anche come Carta Nazionale dei Servizi (TS/Cns).
		3.2.7.4	Conoscere le norme relative all'obbligo di trasmissione telematica dei dati delle ricette.
		3.2.7.5	Descrivere i riferimenti normativi sulle: • Linee Guida del garante della privacy in tema di FSE • Linee Guida del garante della privacy in tema di referti online
	3.2.8 Giustizia digitale	3.2.8.1	Definire il concetto di giustizia digitale.
		3.2.8.2	Conoscere e saper elencare i servizi telematici a disposizione di cittadini e imprese nell'area della giustizia civile.
		3.2.8.3	Saper descrivere il Processo Civile Telematico (PCT) e le relative procedure attivabili.
		3.2.8.4	Determinare il miglioramento del processo penale, dalla fase investigativa al momento dell'esecuzione penale.

Sezione	Tema	Rif.	Argomento
		3.2.8.5	Saper indicare i criteri costituenti i futuri sistemi della giustizia penale, prevalentemente web-based, unificati ed omogenei, con basi dati di livello distrettuale o nazionale e le loro principali linee d'azione.
		3.2.8.6	Saper elencare le linee d'azione prioritarie e gli obiettivi primari per le infrastrutture della giustizia digitale.
3.3 Infrastrutture e Sicurezza	3.3.1 Il Sistema Pubblico di Connettività (SPC)	3.3.1.1	Definire le caratteristiche del Sistema Pubblico di Connettività (SPC).
		3.3.1.2	Definire il concetto di cooperazione applicativa dei sistemi informatici della pubblica amministrazione.
	3.3.2 Il cloud computing	3.3.2.1	Conoscere il significato e l'utilizzo del cloud computing
		3.3.2.2	Saper elencare i riferimenti a livello comunitario e i benefici derivanti dal cloud computing.
	3.3.4 La continuità operativa	3.3.4.1	Definire la continuità operativa e il disaster recovery.
		3.3.4.2	Descrivere le linee guida per il disaster recovery per la PA.
		3.3.4.3	Saper utilizzare lo strumento di autovalutazione per la continuità operativa della PA, sviluppato dall'AgID.
		3.3.4.4	Definire il Piano per la Continuità Operativa (PCO), secondo il disposto normativo vigente e il relativo ruolo dell' AgID.

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.

AICA
Associazione Italiana per l'Informatica ed il Calcolo Automatico

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 (CAdES, 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 disposizioni 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
		4.1.4.12	Saper descrivere la differenza tra i certificati di attributo PKC e gli Attribute Certificate (AC).
4.2 Documento Informatico	4.2.1 Formazione e gestione dei documenti informatici	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 alla regole tecniche vigenti.
		4.2.1.4	Determinare le varie modalità con le quali è formato un documento informatico, secondo le regole tecniche vigenti.
	4.2.2 Immodificabilità dei documenti informatici	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.
		4.2.2.2	Definire il concetto di impronta di un documento informatico e le procedure per saperla calcolare.
	4.2.3 Duplicati, copie ed estratti di documenti informatici e analogici	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, immodificabilità 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 segnature 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 immodificabile durante le fasi della gestione documentale di tenuta, accesso e conservazione.
		4.3.1.6	Determinare le diverse modalità per rendere immodificabile 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	Definireil 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.