

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.



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.

