CORSO VALORE PA 2026

PA digitale e intelligente: governare dati, cybersicurezza e intelligenza artificiale

Area tematica	Documenti e dati digitali - Produzione, gestione e conservazione dei documenti digitali - Sviluppo delle banche dati nazionali, sistemi di autenticazione online, big data, transizione digitale e sicurezza informatica.
Durata del corso	50 ore, articolate in n. 8 moduli
Descrizione del corso	Il percorso formativo affronta in modo dettagliato molteplici aspetti inerenti alla transizione digitale della Pubblica Amministrazione. L'approfondimento dei temi della produzione, gestione e conservazione dei documenti informatici procederà di concerto con un'analisi critica dei ruoli, delle competenze, delle attività, dei processi e dei procedimenti strumentali al raggiungimento degli obiettivi strategici della PA digitale. Si illustreranno gli aspetti salienti dell'Agenda digitale e del Piano Triennale per l'informatica nella pubblica amministrazione, con specifici approfondimenti sugli strumenti operativi (documento informatico, firme elettroniche e servizi fiduciari nel quadro eIDAS 2.0, identità digitale ed EUDI Wallet, PEC e domicilio informatico, protocollo informatico, cloud computing, archiviazione e conservazione, sistemi di autenticazione e servizi online), sulla cybersecurity e sugli adempimenti NIS2, nonché sull'Intelligenza artificiale, anche generativa, e sul quadro europeo dell'AI Act. Il corso approfondirà inoltre Open Data, banche dati di interesse pubblico, riuso e licenze dei contenuti digitali, protezione dei dati personali e comunicazione istituzionale nell'era dell'IA. Ciascun modulo integrerà una sezione dedicata alla illustrazione e discussione di casi pratici ed esempi operativi utili all'applicazione alle situazioni reali delle nozioni e degli strumenti illustrati.

Obiettivi formativi del corso	Il corso è rivolto a far acquisire conoscenze e competenze funzionali al miglioramento delle performance di efficienza, efficacia e semplificazione nel processo di transizione digitale della PA. In particolare, gli obiettivi del corso sono: • Sviluppare capacità progettuali utili a incentivare i cambiamenti operativi interni agli enti pubblici secondo i principi dell'Agenda digitale e dell'ultimo Piano Triennale per l'informatica nella pubblica amministrazione; • Sviluppare competenze relative alla produzione, gestione e conservazione del documento informatico, con specifici approfondimenti sul suo valore giuridico e sulla corretta conservazione digitale dell'archivio dell'ente; • Offrire soluzioni operative su come formare e gestire il fascicolo elettronico nel passaggio dal cartaceo al digitale, anche attraverso la reingegnerizzazione dei flussi documentali; • Proporre soluzioni operative rivolte alla predisposizione dei servizi online dell'ente, con specifici approfondimenti in materia di accessibilità, cloud computing, identità digitale europea ed EUDI Wallet, comunicazione digitale; • Sviluppare un'adeguata consapevolezza sui rischi relativi alla sicurezza informatica, con particolare attenzione agli adempimenti NIS2, alla governance del rischio e alla gestione degli incidenti, proponendo strategie e misure preventive finalizzate a una protezione sicura e resiliente dei dati dell'organizzazione; • Fornire competenze sui possibili impieghi dell'Intelligenza Artificiale, anche generativa, a supporto dell'attività amministrativa, approfondendo il quadro dell'AI Act, l'AI literacy, la supervisione umana, la FRIA nei casi previsti, le garanzie procedimentali, l'explainability e la trasparenza rafforzata del processo decisionale; • Illustrare le corrette procedure da adottare nel trattamento dei dati personali all'interno dell'ente e fornire criteri operativi per il riuso dei dati, la gestione delle licenze e l'impiego responsabile dei contenuti digitali.
Obiettivi strategici	Gestire e organizzare efficacemente le banche dati in possesso di ciascuna PA
Indicatori di outcome:	Aumento del livello di digitalizzazione della PA di appartenenza

Coordinatore del corso e contatti	Prof. Gianmarco Gometz (gometz@unica.it)
Sito web	https://web.unica.it/unica/page/it/corsi_valore_pa_inps_20212022_dipartimento_di_giurisprudenza
Soggetto proponente	Università degli Studi di Cagliari - Dipartimento di Giurisprudenza, Via Sant'Ignazio, 17 - 09123 Cagliari – tel. +39 070 6753044; +39 070 6753820

PROGRAMMA DETTAGLIATO

MODULO 1: GOVERNARE LA TRASFORMAZIONE DIGITALE: REGOLE, RUOLI E RESPONSABILITÀ NELLA PA

Obiettivi: il modulo si propone di favorire una comprensione completa e approfondita della transizione al digitale nella Pubblica Amministrazione. Saranno esplorati i principi e la struttura del Codice dell'Amministrazione Digitale (CAD) e il ruolo fondamentale dell'Agenzia per l'Italia Digitale (AgID) nella promozione e coordinamento della digitalizzazione. Verrà analizzato il nuovo art. 18-bis del CAD riguardante le sanzioni in caso di violazione degli obblighi riguardanti la transizione digitale. Sarà esaminato il Piano Triennale per l'Informatica nella Pubblica Amministrazione, definendo gli obiettivi strategici per la digitalizzazione delle attività amministrative. Saranno trattati il ruolo del Difensore Civico per il Digitale, del Responsabile per la Transizione al Digitale (RTD) e del Referente per la cybersicurezza, delineando le loro funzioni e responsabilità. Infine, saranno illustrate le nuove competenze richieste per l'adozione di soluzioni di IA nella pubblica amministrazione.

Argomenti:

- Il Codice dell'Amministrazione Digitale (CAD): struttura e principi generali
- La carta della cittadinanza digitale
- L'agenzia per l'Italia Digitale: ruolo, funzioni e competenze
- Le sanzioni in caso di violazione degli obblighi di transizione digitale: il nuovo art. 18-bis CAD

- Il difensore civico per il digitale: ruoli e funzioni
- L'ufficio transizione al digitale: aspetti organizzativi
- Il Responsabile per la Transizione al Digitale (RTD): nomina, ruolo e rapporto con gli altri soggetti coinvolti
- Il Piano triennale per l'informatica nella pubblica amministrazione: dalla transizione al digitale all'impiego dell'intelligenza artificiale nella PA
- Le nuove competenze, la governance interna e l'AI literacy per l'adozione responsabile dell'Intelligenza Artificiale nella Pubblica Amministrazione
- I nuovi adempimenti previsti dalla Direttiva NIS2 e il referente per la cybersicurezza
- Casi pratici, esempi e modelli operativi

MODULO 2: IL DOCUMENTO DIGITALE CHE VALE: FIRME, PROTOCOLLO, IDENTITÀ E PROVA

Obiettivi: Il modulo ha l'obiettivo di favorire una completa comprensione del documento informatico nella Pubblica Amministrazione. Saranno esaminate le caratteristiche principali e il valore giuridico del documento elettronico, con un focus sulla sua conservazione nel ciclo di vita. Il modulo seguirà le Linee Guida AgID per la formazione, gestione e conservazione dei documenti informatici, analizzando le diverse fasi e le criticità coinvolte nella formazione del documento informatico. Sarà esplorato il ruolo dei formati del documento e dei metadati nella gestione documentale. Le firme elettroniche e i servizi fiduciari saranno studiati alla luce del quadro eIDAS ed eIDAS 2.0, con specifica attenzione all'identità digitale europea e all'European Digital Identity Wallet (EUDI Wallet). Saranno analizzati la marca temporale, la validazione e il riferimento temporale per garantire l'integrità temporale dei documenti digitali. Il valore sostanziale e probatorio del documento informatico sarà valutato fornendo indicazioni per garantirne l'autenticità e l'affidabilità. Infine, saranno esaminate le pratiche per la realizzazione e gestione di copie e duplicati dei documenti informatici.

Argomenti:

- Le principali caratteristiche e valore giuridico del documento elettronico nella PA: valore giuridico e ciclo della conservazione

- Il ciclo di vita del documento nelle Linee Guida AgID sulla formazione, gestione e conservazione dei documenti informatici
- Formazione del documento informatico: analisi delle fasi e criticità
- I formati del documento informatico e il ruolo dei metadati nella gestione documentale
- Le firme elettroniche e i servizi fiduciari nel quadro eIDAS ed eIDAS 2.0; identità digitale europea ed European Digital Identity Wallet (EUDI Wallet)
- Marca temporale, validazione e riferimento temporale
- Il valore sostanziale e probatorio del documento digitale
- Realizzazione e gestione delle copie e dei duplicati del documento informatico
- Istanze e dichiarazioni presentate alle pubbliche amministrazioni per via telematica
- Introduzione al sistema di gestione dei flussi documentali e le nuove frontiere della gestione documentale: casi d'uso e applicazione pratica dell'intelligenza artificiale
- Casi pratici, esempi e modelli operativi

MODULO 3: DAL PROTOCOLLO AL CLOUD: FLUSSI DOCUMENTALI, FASCICOLI E CONSERVAZIONE DIGITALE

Obiettivi: il modulo ha l'obiettivo di favorire una comprensione completa e dettagliata della gestione dei flussi documentali, dei fascicoli elettronici e della conservazione dei documenti informatici. Saranno esaminate le principali caratteristiche del documento elettronico con particolare attenzione al suo ciclo di conservazione. Le Linee Guida dell'Agenzia per l'Italia Digitale (AgID) sul ciclo di vita del documento informatico saranno esaminate per garantire una aggregazione e una fascicolazione coerente ed efficace dei documenti digitali, con un focus sul ruolo dei metadati nella gestione documentale. Particolare rilievo sarà dato alle tecniche per garantire la tracciabilità del documento digitale e al *cloud computing* nella P.A. Infine, il modulo fornirà istruzioni circa la conservazione adeguata delle copie e dei duplicati dei documenti informatici.

Argomenti:

- Le regole tecniche sulla gestione documentale (Linee Guida AgID)
- Gli strumenti operativi di gestione documentale: il protocollo informatico e il registro giornaliero di protocollo

- La classificazione dei documenti informatici
- Fascicolazione e aggregazioni documentali
- Il responsabile della gestione documentale e adempimenti organizzativi della P.A.: il manuale della gestione documentale
- Il sistema di conservazione dei documenti in ambito pubblico
- Il Responsabile della conservazione: designazione, ruolo e responsabilità
- Il responsabile del servizio di conservazione e il contratto di outsourcing.
- I criteri per la fornitura dei servizi di conservazione dei documenti informatici
- Introduzione alle nuove tecnologie sviluppate sulla raccolta e trattamento di grandi quantità di dati
- Modelli di implementazione e tipologie di cloud
- Le nuove regole del cloud nella P.A.
- Casi pratici, esempi e modelli operativi

MODULO 4: PA CYBER-RESILIENTE: SICUREZZA, PREVENZIONE E GESTIONE DEGLI INCIDENTI

Obiettivi: Il modulo ha l'obiettivo di favorire una completa comprensione della cybersecurity nella Pubblica Amministrazione, con particolare attenzione alla resilienza dei sistemi e alla gestione organizzativa del rischio. Saranno analizzati gli obblighi derivanti dal quadro NIS2, le responsabilità dei soggetti coinvolti, la gestione sicura dell'infrastruttura tecnologica e dei sistemi informativi, le vulnerabilità e le relative contromisure. Il modulo approfondirà le misure di sicurezza, la definizione e l'attuazione delle politiche interne, gli standard, le procedure e la documentazione, con specifico rilievo alla gestione e notifica degli incidenti, al monitoraggio e al rapporto con le autorità e le strutture nazionali competenti in materia di cybersicurezza.

Argomenti:

- Concetti generali di Information e Cybersecurity
- La gestione dell'infrastruttura tecnologica e dei sistemi informativi
- Vulnerabilità dei sistemi e contromisure;
- Misure di sicurezza ICT, gestione del rischio e adempimenti operativi previsti dal quadro NIS2
- Governance della cybersicurezza nella PA: ruoli, responsabilità, politiche interne

e referente per la cybersicurezza
- L'implementazione delle politiche di sicurezza
- Standard, procedure e documentazione
- Gestione e notifica degli incidenti; coordinamento con ACN e CSIRT Italia
- Monitoraggio e controllo
- Casi pratici, esempi e modelli operativi

MODULO 5: PROTEGGERE I DATI NELLA PA DIGITALE: PRIVACY, ACCOUNTABILITY E SICUREZZA

Obiettivi: Il modulo si propone di favorire una comprensione completa e dettagliata delle normative sulla protezione dei dati personali nei sistemi di gestione documentale. Saranno esaminate le principali disposizioni normative del Regolamento Generale sulla Protezione dei Dati (RGPD) e del D. Lgs. 196/2003, così come modificato dal D. Lgs. 101/2018, riguardanti il trattamento dei dati personali nell'ambito della Pubblica Amministrazione. saranno analizzati il ruolo e le responsabilità del Responsabile della Protezione dei Dati (RPD-DPO), insieme ai principali adempimenti del RGPD, tra cui il consenso degli interessati, la gestione delle richieste degli interessati e la notifica delle violazioni dei dati. Saranno esaminati i diritti conferiti agli interessati dal RGPD e le misure di ricorso, responsabilità e sanzioni in caso di violazione dei dati personali. Il modulo fornirà indicazioni sulle misure di sicurezza necessarie per proteggere i dati personali e sulle modalità di scambio di dati tra amministrazioni pubbliche, garantendo il rispetto delle normative sulla privacy.

Argomenti:

- Analisi degli aspetti generali della nuova disciplina in materia di trattamento dei dati personali prevista dal Regolamento (UE) 2016/679 "Regolamento Generale sulla Protezione dei Dati – RGPD) e del D. Lgs. 196/2003 (così come modificato dal D. Lgs. 101/2018)
- Il Responsabile della Protezione dei Dati (RPD-DPO)
- I principali adempimenti del Regolamento (UE) 2016/679
- Diritti dell'interessato
- Mezzi di ricorso, Responsabilità e Sanzioni
- Misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni

pubbliche
- Casi pratici, esempi e modelli operativi

MODULO 6: DATI E CONTENUTI NELLA PA DIGITALE: OPEN DATA, LICENZE E INTELLIGENZA ARTIFICIALE

Obiettivi: il modulo ha l'obiettivo di favorire una comprensione approfondita della gestione e valorizzazione dei dati e dei contenuti digitali della Pubblica Amministrazione, con particolare attenzione alle condizioni giuridiche per la loro condivisione e il loro riutilizzo. Saranno trattati il patrimonio informativo pubblico, gli Open Data, le banche dati e i principali modelli di licenza, mettendo in evidenza i profili di titolarità e responsabilità.
Il modulo approfondirà inoltre i rapporti tra patrimonio digitale pubblico, diritto d'autore e tutela delle banche dati, nonché le regole applicabili all'utilizzo di software e contenuti di terzi da parte delle amministrazioni.
Particolare attenzione sarà infine dedicata all'intelligenza artificiale generativa, alle questioni relative all'impiego di contenuti protetti come input e alla qualificazione, verifica e riutilizzo degli output generati mediante sistemi di IA.

Argomenti:

- Il patrimonio informativo e i contenuti digitali della Pubblica Amministrazione
- I sistemi informativi della PA: Piattaforma Digitale Nazionale Dati e basi di dati di interesse nazionale
- Open Data e riuso dell'informazione del settore pubblico
- Licenze per la condivisione e il riutilizzo dei dati: profili tecnico-giuridici
- Titolarità e responsabilità sul patrimonio informativo e sui contenuti digitali della PA
- Diritto d'autore, documenti amministrativi e contenuti digitali della Pubblica Amministrazione
- La tutela giuridica delle banche dati
- Software proprietario, software open source e riuso nella Pubblica Amministrazione
- Big Data, condivisione dei dati e protezione dei dati personali
- Intelligenza artificiale generativa, diritto d'autore e contenuti digitali: input,

output e riutilizzo
- Casi pratici, esempi e modelli operativi

MODULO 7: LA PA ALGORITMICA: DECISIONI, TRASPARENZA E RESPONSABILITÀ NELL'ERA DELL'IA

Obiettivi: Il modulo ha l'obiettivo di favorire una comprensione approfondita del processo di algoritmizzazione dell'attività amministrativa e dell'impiego dell'Intelligenza Artificiale nella Pubblica Amministrazione. Verrà esaminato il quadro dell'AI Act, con particolare attenzione agli obblighi delle amministrazioni in qualità di deployer, all'AI literacy, alla governance interna, alla supervisione umana e, nei casi previsti, alla valutazione d'impatto sui diritti fondamentali (FRIA). Saranno inoltre approfonditi gli impieghi dell'IA generativa nelle attività di redazione, sintesi, ricerca, assistenza all'utenza e supporto istruttorio, evidenziando i rischi connessi alle allucinazioni, all'inserimento di dati personali o riservati e alla necessità di verifica umana degli output. Attraverso casi studio e casistica giurisprudenziale saranno infine esaminati i limiti dell'automazione nelle attività istruttorie e decisionali e le garanzie di conoscibilità, accesso, explainability e trasparenza rafforzata.

Argomenti:

- L'AI Act nella Pubblica Amministrazione: principi, classificazione del rischio, obblighi e responsabilità della PA come deployer
- Strategia italiana per l'Intelligenza Artificiale e indirizzi nazionali per l'impiego dell'IA nella Pubblica Amministrazione
- AI literacy, governance interna e competenze organizzative per l'impiego responsabile dell'IA
- Il ricorso agli algoritmi nell'attività amministrativa: attività decisoria e provvedimenti automatizzati
- Uso degli algoritmi nelle attività istruttorie e nell'accertamento dei fatti complessi
- L'evoluzione giurisprudenziale sull'impiego degli algoritmi nell'attività discrezionale
- Adozione di sistemi di IA nella PA: valutazione del rischio, supervisione umana e accountability

- La valutazione d'impatto sui diritti fondamentali (FRIA) nei casi previsti dall'AI Act
- Intelligenza artificiale generativa nella PA: casi d'uso per redazione, sintesi, ricerca, assistenza all'utenza e supporto istruttorio
- Rischi dell'IA generativa: allucinazioni, dati personali e riservati, affidabilità delle fonti e verifica umana degli output
- Accesso agli «atti algoritmici», explainability, conoscibilità e nuove forme di «trasparenza rafforzata»
- Casi pratici, esempi e modelli operativi

MODULO 8: COMUNICARE LA PA NELL'ERA DELL'IA: SOCIAL MEDIA, CHATBOT E CONTENUTI DIGITALI

Obiettivi: Il modulo analizza l'evoluzione della comunicazione istituzionale della Pubblica Amministrazione nell'ambiente digitale, mantenendo il riferimento ai principi della comunicazione pubblica e alle forme di comunicazione interna ed esterna. Saranno approfondite le implicazioni giuridiche dell'utilizzo dei social media, dei chatbot, degli assistenti virtuali e degli strumenti di intelligenza artificiale generativa. Particolare attenzione sarà dedicata ai doveri di comportamento dei dipendenti pubblici, alla protezione dei dati personali, al diritto d'autore, all'affidabilità dei contenuti e alla necessità di verifica e supervisione umana. L'obiettivo è fornire criteri operativi per una comunicazione digitale efficace, responsabile e coerente con gli obblighi della PA.

Argomenti:

- La comunicazione pubblica nell'ambiente digitale: principi, disciplina e rapporto con cittadini e utenti
- Comunicazione interna ed esterna nella PA; account social istituzionali e interazione con l'utenza
- Social network e doveri di comportamento dei dipendenti pubblici: profili istituzionali e profili personali
- Comunicazione digitale tra accountability, trasparenza, protezione dei dati e riservatezza
- Immagini, testi, video e contenuti di terzi nella comunicazione istituzionale: diritto d'autore e licenze
- Chatbot, assistenti virtuali e IA generativa per la produzione e diffusione di

contenuti istituzionali
- Allucinazioni, deepfake e manipolazione dell'informazione: verifica delle fonti, affidabilità e supervisione umana
- Responsabilità, rischi e buone pratiche nell'uso dei nuovi strumenti digitali; casi pratici ed esempi operativi

Prova finale di valutazione dell'apprendimento (ore 16:00-18:00)