Unicollege
SSML Mantova
Istituto ad Ordinamento Universitario
D.M. 31/07/2003, G.U. n. 201 30/08/2003

SSML di Mantova
Via G.Rippa, 2
46100 Mantova (MN)
Tel. +39 0376 368481
Fax +39 0376 368481

master.mn@unicollege.it

BANDO DI CONCORSO PER L'AMMISSIONE AL CORSO PER MASTER DI I LIVELLO IN

"CYBER SECURITY & DATA PROTECTION"

A.A. 2016/17

I EDIZIONE

1 – ISTITUZIONE

La Scuola Superiore per Mediatori Linguistici Unicollege di Mantova (di seguito SSML) istituisce per l'A.A. 2016/2017, la I edizione del Corso per Master di I Livello in CIBER SECURITY & DATA PROTECTION.

2 – CARATTERISTICHE DEL CORSO

1. Numero minimo e massimo di posti disponibili

Il corso sarà attivato previo raggiungimento di almeno 20 (venti) partecipanti.
Il numero massimo di posti disponibili è stato fissato a 35 (trentacinque) unità.

2. Durata, crediti formativi e titolo di studio rilasciato

Il Corso per Master in Cyber Security & Data Protection è un corso di perfezionamento della durata di un anno alla conclusione del quale, previo superamento di un esame finale, si rilascia il titolo di Master di I livello.

Il Corso avrà una durata di 1.500 ore corrispondenti a 60 Crediti Formativi (CF) ai sensi del D.M. 22/10/2004 n. 270.

3. Quota di iscrizione

La quota di iscrizione è pari a € 4.800,00 di cui € 4.000,00 finanziati da Regione Lombardia per residenti o domiciliati in Regione, a cui andranno aggiunti € 16,00 di marca da bollo.
Per le modalità di pagamento si veda ai commi 2 e 3 del punto 4.

SSML di Mantova
Via G.Rippa, 2
46100 Mantova (MN)
Tel. +39 0376 368481
Fax +39 0376 368481

master.mn@unicollege.it

3 – DESCRIZIONE DEL CORSO

Il Corso per Master in Cyber Security & Data Protection si propone di fornire un'adeguata formazione a coloro che, in virtù della loro attività, sono determinati a migliorare e aggiornare le proprie conoscenze, modelli e metodologie per la prevenzione dei fenomeni criminosi in ambito informatico, fornendo una panoramica sulle più recenti strategie di contrasto a livello internazionale. Il percorso del Master in Cyber Security e Data Protection è principalmente rivolto a professionisti sia della Pubblica Amministrazione che del settore privato, nonché a laureati interessati a perfezionare la propria professionalità nel campo della sicurezza informatica e della prevenzione di furti o attacchi ai sistemi in uso.

1. A chi è rivolto

Gli ideali destinatari del Corso per Master in Cyber Security e Data Protection sono individuati tra le seguenti categorie professionali:

- operatori di Polizia Postale;
- consulenti e liberi professionisti di area informatica;
- responsabili aziendali di IT;
- laureati in informatica;
- funzionari delle PA in area IT;
- membri delle forze dell'ordine.

Sono, altresì, destinatari del Corso tutti coloro che, in possesso di solide conoscenze informatiche, sono interessati ad acquisire gli strumenti necessari per la corretta gestione e applicazione della normativa europea relativa alla sicurezza informatica .

2. Obiettivi

Gli obiettivi del Corso per Master in Cyber Security e Data Protection possono essere riassunti nei seguenti punti:

1. acquisire/migliorare la capacità di valutazione dei rischi del sistema informativo, rispetto a minacce e profili di vulnerabilità;
2. introdurre standard di sicurezza e programmare interventi per ridurre i rischi e/o eliminarli;
3. applicare principi di programmazione sicura nello sviluppo di architetture sicure;
4. applicare metodi di rilevazione e prevenzione delle intrusioni nella rete;
5. applicare tecniche di protezione crittografica;
6. approfondire gli aspetti legati alle recenti normative Europee (Direttiva NIS), e alle procedure di certificazione;
7. adeguare metodologie e comportamenti alle Best Practice internazionali.

SSML di Mantova
Via G.Rippa, 2
46100 Mantova (MN)
Tel. +39 0376 368481
Fax +39 0376 368481

master.mn@unicollege.it

3. Sbocchi professionali

Il Corso per Master in Cyber Security e Data Protection fornisce competenze specialistiche adeguate alle seguenti figure:

- operatori informatici impiegati in società ed enti pubblici e privati che utilizzano reti informatiche di dimensioni medie e grandi;
- consulenti e liberi professionisti di area informatica;
- profili quali IT Manager e Network Specialist;
- responsabili di analisi della sicurezza e di applicazioni e sistemi informatici
- responsabili di progettazione e realizzazione di applicazioni e sistemi informatici sicuri
- responsabili di analisi di attacchi informatici
- Consulenti Tecnici di Parte (CTP) e d'Ufficio (CTU)

4. Frequenza e modalità di insegnamento

Gli insegnamenti saranno impartiti tramite lezioni frontali, con il supporto di strumentazione audio e video. La frequenza alle lezioni è obbligatoria per almeno il 75% delle ore tranne che per i moduli 1 e 2 oggetto di finanziamento di Regione Lombardia, per i quali è necessaria una presenza minima del 90% delle ore dei moduli stessi. Eventuali richieste di esonero dalla frequenza verranno valutate dall'Ufficio Master caso per caso.

5. Durata e sede del corso

Il Corso per Master in Cyber Security e Data Protection ha durata annuale. Le lezioni si svolgeranno secondo il calendario che verrà predisposto dalla Segreteria e comunicato agli studenti iscritti prima dell'inizio delle lezioni.
Le lezioni si svolgeranno presso la sede della SSML Unicollege di Mantova, in via G. Rippa, 2 o presso la sede di Milano di Adiuva S.r.l., in p.le Cadorna 10.

6. Descrizione dei contenuti

1. Modulo 1.1: ICT Security Specialist - Effettuare la revisione del sistema IT in uso

Sicurezza Informatica: *Metodi di rilevazione e prevenzione delle intrusioni di rete. Crittografia. Sicurezza dei sistemi, delle reti, dei programmi. Crittoanalisi e hacking. Modelli comportamentali e principi legali, di networking, sistemistici, di programmazione e design. Basi per la valutazione del livello di sicurezza di un sistema ICT. Modelli di sviluppo dei processi e con configuration management.*

Sistemi di prevenzione degli attacchi alla rete: *Procedure per la sicurezza dei dati. Tecniche per l'analisi della sicurezza degli apparati informatici. Guasti HW, malfunzionamenti SW e accesso dati. Affidabilità dei sistemi. Autenticazione degli utenti: password, PIN, fingerprint. Concetto di Integrità del sistema. Minacce e Difese: virus/worm, troyan, keylogger, backdoor, rootkit.*

SSML di Mantova
Via G.Rippa, 2
46100 Mantova (MN)
Tel. +39 0376 368481
Fax +39 0376 368481

master.mn@unicollege.it

2. Modulo 1.2: ICT Security Specialist - Valutare il grado di sicurezza del sistema sviluppato

Principi di programmazione sicura: *Fondamenti delle architetture dei sistemi informativi (N.Tier Application, Cloud, Internet Data Center ICD, Hosting/Housing, Apps, etc), dei principali linguaggi di programmazione. Paradigmi di programmazione. I requisiti di un sistema IT software sicuro e nel rispetto delle normative sulla Privacy DLgs 196/2003 e succ. I Principi di programmazione Object Oriented OOP e Service Oriented SOA ed i principali livelli di una applicazione IT moderna web/mobile IoT. Le principali fasi di un modello di sviluppo software iterativo (Analisi, Disegno, Agile & Scrum).*

Sicurezza dei sistemi operativi: *Procedure adatte a garantire la necessaria sicurezza nei sistemi informativi desktop, mobile e server, e nelle reti cablate e senza fili. Strumenti di controllo degli accessi e di aggiornamento automatico di un sistema operativo.*

Sicurezza delle applicazioni web: *Le parti principali di un'applicazione WEB ed i protocolli, livelli, Tier. Controllo degli accessi a funzioni e partizioni di dati/informazioni. Comunicazione e registrazione dei dati crittografata (certificati, crittografia dei dati, visibilità Internet, Extranet, Intranet, livelli di accesso). Principi di progettazione di un sistema informativo Web/App per la sicurezza. Riduzione/prevenzione dei rischi indotti da minacce e vulnerabilità. Valutazione del livello di sicurezza di un'applicazione web ed interventi pratici per aumentarla. Applicazione di tecniche di protezione crittografica.*

Sicurezza delle basi di dati: *Regole per la configurazione dei ruoli e permessi; servizi per l'accesso ad una base dati SQL o NoSQL. Archivi documentali. Strumenti di controllo degli accessi alle basi di dati. Tecniche di valutazione del rischio informatico. Modelli di progettazione e valutazione di affidabilità, disponibilità, correttezza, disaster recovery di applicazioni ICT. Gestione della dislocazione dei dati, backup e recovery, e gestione Incident & Problems (Best Pratices ITIL, Normative ISO, DLgs 231/01). Sicurezza delle basi di dati di supporto alle applicazioni software web e mobile, sicurezza del trasporto/consegna e garanzia autenticità e inviolabilità del contenuto. Valutazione del grado di sicurezza informatica del sistema sviluppato. Database cifrati. SQL Injection. Trattamento dati sensibili.*

Sicurezza delle reti senza fili: *Vulnerabilità comparata con rete cablate. Strategie di difesa da attacchi e intrusioni via etere.*

SSML di Mantova
Via G.Rippa, 2
46100 Mantova (MN)
Tel. +39 0376 368481
Fax +39 0376 368481

master.mn@unicollege.it

3. Modulo 2.1: Network Specialist – Gestire gli apparati e le connessioni di rete

Apparati di rete e cablaggio strutturato: *Procedure di qualità per reti cablate. Panoramica dello stato dell'arte. Casistica*

Comunicazioni IP: *Protocolli di comunicazione IP. Gli stack protocollari : IPv4 e IPv6, ICMP, TCP/UDP, DNS, FTP/HTTP/SMTP/POP3/IMAP, SSH/SSL/TLS, etc. Apparati e Network element.*

Modem e modulazione: *Dispositivi di modulazione/demodulazione. Apparati e Network element.*

Principi e norme sulle reti: *Standard di funzionamento delle reti cablate e senza fili. Panoramica dello stato dell'arte. Casistica*

Protocolli di rete non-IP: *Protocolli di comunicazione non-IP. Apparati Ethernet, le reti ATM, SDH, PDH Radio e cablate.*

Protocolli per reti senza fili: *Dispositivi di comunicazione in rete: i diversi standard. Estensione della copertura delle reti wireless. Tecnologie NFC e Bluethooth.*

Reti Ethernet: *Protocolli, livelli e modalità di trasporto. SSL/TLS, SSH. SMIME, PEC, con laboratorio e/o IPSec. WiFi and Bluetooth Security.*

Reti locali virtuali (VLAN) e segmentazione: *Dispositivi per reti locali virtuali (VLAN) o segmentate. Livelli di accesso alle reti. Dimensionamento della banda (Server Area Network SAN, LAN, WAN, DMZ). Interconnessioni tra i diversi livelli di network mediante NAT.*

Sistemi di instradamento di pacchetti di comunicazione: *Dispositivi di instradamento (router), di protezione e controllo degli accessi in ingresso ed uscita (Firewall, Internet Gateway, Web-Filtering). Gestione degli apparati e delle connessioni di rete. Reti pubbliche e private, NAT/PAT, port forwarding, VLAN.*

4. Modulo 2.2: Network Specialist – Gestire i servizi di rete a livello applicativo

Principi di gestione della posta elettronica: *Procedure di configurazione della posta elettronica, sia lato client che lato server. Crittografia dei contenuti (dati personali, sensibili, controllo autorizzazioni di accesso). Firma digitale, PEC e gestione dell'Archiviazione ottica sostitutiva. Soluzioni e casi. Practice policy per la gestione della posta elettronica aziendale e problematiche di accessibilità in mobilità o fuori dalla rete aziendale.*

Sistemi di sicurezza della rete: *Procedure di configurazione di risorse condivise, software ed apparati. Firewall e antivirus. Stato dell'arte e soluzioni.*

SSML di Mantova
Via G.Rippa, 2
46100 Mantova (MN)
Tel. +39 0376 368481
Fax +39 0376 368481

master.mn@unicollege.it

Sistemi Operativi: *Procedure di sicurezza della rete sui sistemi interni e pubblicati, gestione del controllo degli accessi remoti, soluzioni di blocco IP. Introduzione alle tecnologie Cloud (storage, computing), paradigmi di cloud services. Aspetti generali di sicurezza nelle tecnologie cloud-based. Mobile OS e sicurezza: struttura e caratteristiche dei SO più diffusi (Android, iOS, Windows). Mobile code: modelli di distribuzione delle applicazioni, problematiche e rischi (i.e. integrità e autenticità del codice), pratiche comuni (mutuate/ereditate da tecnologie precedenti - isolation/sandboxing). Malware detection: tecniche di ispezione e riconoscimento del codice malevolo, panoramica sul numero e i tipi di malware per dispositivi mobili. Modelli di sicurezza: access control, usage control e history-based security (specifica e prevenzione dei comportamenti indesiderati), language-based security. NFC e Host-based Card Emulation, Remote Attestation, Trusted Execution Environments. Caso di studio/progetto: Soluzioni per il paradigma Bring Your Own Device (BYOD) o soluzioni per il mobile/proximity payment.*

Sistemi Operativi per la condivisione di risorse in rete: *Applicare tecniche di soluzione dei problemi di un sistema operativo per la raccolta, la condivisione ed il backup dei dati. Network Area Storage e Server Area Storage. Restrizione e controllo degli accessi.*

VOIP e qualità del servizio di comunicazione: *Dispositivi di integrazione fonia/dati. Priorità, quality of service, virtualizzazione di numerazioni geografiche. Modello di rete Voip: esempi di soluzioni open-source per centralini Voip e non Voip, installabili anche in cloud (Asterisk). Problematiche dei sistemi di video conferenza.*

World Wide Web: *Servizi web. Soluzioni web sicure (progettazione, livelli del sistema, principi di Model View Control MVC). Disegno di soluzioni web/mobile. Scelta delle principali componenti HW/SW e dell'infrastruttura di produzione (infrastruttura cloud, virtualizzazione, IDC tradizionale). Gestire i servizi di rete a livello applicativo. Introduzione al Web: protocollo http, modello client –server, HTML, cookies, Server-side Scripting (PHP), DOM e Client-side Scripting, Cross-site Scripting, DB Security and SQL-injection. Browser-based Security protocols: SAML SSO , OpenID, OAuth, Security of HTML5. JavaScript injection.*

5. Modulo 2.3: Network Specialist – Verificare la qualità dei servizi nelle reti informatiche

Elementi di gestione del servizio IT: *Metodologie di diagnosi del funzionamento di una rete. Panoramica dello stato dell'arte. Casistica.*

Modelli di gestione delle reti: *Metodologie di gestione delle reti. Panoramica dello stato dell'arte. Casistica.*

Normativa sulla tutela della salute e sicurezza dei lavoratori in tutti i settori di attività privati o pubblici: *Panoramica dello stato dell'arte. Casistica.*

Norme europee salute e sicurezza in ambito IT: *Panoramica dello stato dell'arte. Casistica.*

SSML di Mantova
Via G.Rippa, 2
46100 Mantova (MN)
Tel. +39 0376 368481
Fax +39 0376 368481

master.mn@unicollege.it

Problematiche relative alla gestione delle reti*: Principi di salute e sicurezza nei sistemi IT e loro applicazione. Metodologie di ripristino malfunzionamento di una rete. Panoramica dello stato dell'arte. Casistica.*

Tecniche di pianificazione di attività: *Procedure di gestione del servizio IT. IT Services Management. Gestione delle richieste in ambito IT generate dagli utenti del sistema o dalle situazioni di allarme generate dai sistemi di Monitoring e Facility Management (Intrusion, Disk Space Treshold, etc.).Tecniche di pianificazione di risorse e mezzi per garantire i livelli di servizio SLA contrattualizzati. Organizzazione di piani di crescita. Individuazione di risorse/mezzi aggiuntivi (Capacity Plan) in base alle richieste del business. Verifica della qualità dei servizi nelle reti informatiche. Principi di project management: BWS, Effort/Elapsed Time esource planning. Risk cost.*

6. Modulo 3: Cyber Intelligence

Crittografia e Sicurezza Informatica: *Teoria dell'informazione e concetto di entropia. Cifratura con chiave simmetrica. Funzioni hash. Cifratura a chiave pubblica. Firme e certificati digitali. Social Engineering. Impersonation attacks, furto di identità. Best practice comportamentali. Social networks, user profiling, webtracking.*

7. Modulo 4: Legal Aspects

Informatica Forense: *Introduzione alle problematiche di computer forensic**.** La digital forensic nell'accertamento civilistico (Leggi, Disposizioni per lo Sviluppo Economico, la Semplificazione, la Competitività in materia di Processo Civile, Codice di Procedura Civile, CTU). La Convezione di Budapest e le modifiche al Codice di Procedura Penale. Processo Penale e fasi del procedimento Penale. Verbale d'incarico nella procedura penale. L'accertamento tecnico ripetibile. L'accertamento tecnico irripetibile.*
Determinazione ed analisi del contesto operativo. L'acquisizione delle prove. La non ripudiabilità delle prove acquisite. La catena di custodia. Confini transnazionali dei crimini informatici e problemi di giurisdizione. Strumenti di analisi con licenza commerciale. Strumenti di analisi open source. OSINT. La validità degli strumenti di acquisizione delle prove digitali.

Aspetti legali della Cyber Security: *Dal Safe Harbour al Privacy Shield. Il GDPR (General Data Protection Regulation). Il Regolamento UE 2016/679 e la Direttiva UE 2016/680. Differenze tra Regolamento e Direttiva. Accountability, Privacy by design e Privacy by default, Diritto di accesso, DPIA , Data retention, Diritto all'oblio, One Stop Shop, Trasferimento dati extra UE, Data breach, Sanzioni Amministrative e Penali. DPO (Data Protecion Officer), Registro dei trattamenti, Provvedimento Ammistratori di Sistema, Audit AdS e Consulenza Privacy. La Direttiva UE NIS (Network and Information System) del 2016 e l'Italian Cyber Security Report/Framework 2015. Attuazione della Direttiva 2008/114/CE. Quadro Strategico Nazionale e Piano Nazionale per la protezione cibernetica e la sicurezza informatica. Direttiva 2002/58/CE. DPIA come strumento di valutazione preventiva e permanente del rischio. Il Regolamento UE eIDAS (electronic IDentification Authentication and Signature).*

SSML di Mantova
Via G.Rippa, 2
46100 Mantova (MN)
Tel. +39 0376 368481
Fax +39 0376 368481

master.mn@unicollege.it

8. Modulo 5: Tirocinio

A completamento del percorso formativo è previsto un periodo di tirocinio della durata di 350 ore da svolgersi, previo parere positivo dell'Ufficio Master, presso Società, Enti, Associazioni che operino negli ambiti di interesse trattati durante il Corso.
Il corsista dovrà produrre una relazione sul tirocinio svolto che verrà valutata ai fini del conseguimento del titolo finale.

7. Ufficio di riferimento

Ufficio Master, tel + 39 02 87388760, fax 02 87388730, e-mail master.mn@unicollegessml.it

4 - REQUISITI E MODALITÀ DI ACCESSO

1. Chi può fare domanda

L'ammissione al Corso per Master è subordinata al possesso di almeno un Diploma di Laurea Triennale rilasciato in Italia o titolo equipollente.

I candidati in possesso di un titolo accademico straniero devono far pervenire i documenti utili in originale per consentirne la verifica (titolo corredato di traduzione ufficiale in lingua italiana, con legalizzazione e dichiarazione di valore a cura delle rappresentanze diplomatiche italiane nel Paese in cui il titolo è stato conseguito; quanto sopra al fine del riconoscimento del medesimo per la sola iscrizione al Corso per Master) alla Segreteria, allegando il documento alla Domanda di Iscrizione.

Possono inoltre presentare Domanda di Iscrizione anche coloro che, alla data di scadenza del bando, non abbiano ancora sostenuto l'esame di laurea ma prevedono di essere in possesso di tale titolo accademico entro il giorno dell'inizio previsto del Corso di Master. In questo caso è necessario che tali candidati specifichino la loro condizione nell'apposito campo del modulo della Domanda di Iscrizione. Il modello di autocertificazione del titolo di studio è scaricabile dal sito www.unicollegessml.it.

2. Modalità di Iscrizione al Corso

I candidati potranno iscriversi al Corso per Master fino al 3 marzo 2017.
Per iscriversi al Corso per Master, i candidati dovranno seguire la seguente procedura:

1. scaricare dal sito www.unicollegessml.it il Modulo di Iscrizione al Master di I Livello in Cyber Security e Data Protection, stamparlo e compilarlo in ogni sua parte;

SSML di Mantova
Via G.Rippa, 2
46100 Mantova (MN)
Tel. +39 0376 368481
Fax +39 0376 368481

master.mn@unicollege.it

2. versare entro il 3 marzo 2017 l'acconto di € 300,00 sulla quota di pre-iscrizione non rimborsabile (pari a € 800,00) presso la Segreteria della SSML di Mantova, via G. Rippa, 2, o tramite bonifico utilizzando le seguenti coordinate bancarie:
   Intestatario:
   SSML di Mantova
   IBAN:
   IT 78 C 02008 01600 000104229607
   Causale:
   Iscrizione Master CSDP – Cognome e Nome

3. allegare al Modulo di Iscrizione i seguenti documenti:
- ricevuta di versamento della pre-iscrizione;
- autocertificazione del titolo accademico (modello scaricabile dal sito www.unicollegessml.it);
- 2 foto formato tessera;
- fotocopia di un documento di identità in corso di validità e del codice fiscale dello studente;
- permesso di soggiorno per i cittadini extracomunitari (costituisce titolo valido anche la ricevuta di richiesta di soggiorno rilasciata in posta; sarà responsabilità del candidato inviare alla Segreteria copia del documento originale appena ne sarà in possesso).

4. far pervenire il Modulo di Iscrizione e tutti gli allegati secondo una delle seguenti modalità:
- consegna a mano presso la Segreteria della SSML di Mantova, via G. Rippa, 2, Mantova;
- invio tramite raccomandata con ricevuta di ritorno alla Segreteria della SSML di Mantova, via G. Rippa, 2, Mantova.

5. Procedere al saldo della quota di pre-iscrizione pari a € 500,00 entro il giorno di inizio del Master.

3. Modalità di Pagamento del Corso

I candidati pre-iscritti e accettati sono tenuti a regolarizzare la loro posizione amministrativa secondo le seguenti scadenze:

1. versare entro il 10 marzo 2017 la prima rata di € 2.000,00 con le stesse modalità di pagamento della pre-iscrizione solo se non ammessi al finanziamento di Regione Lombardia.
2. versare entro 30 aprile 2017 il saldo di € 2.000,00 con le stesse modalità di pagamento della pre-iscrizione solo se non ammessi al finanziamento di Regione Lombardia.

SSML di Mantova
Via G.Rippa, 2
46100 Mantova (MN)
Tel. +39 0376 368481
Fax +39 0376 368481

master.mn@unicollege.it

Grazie a una convenzione con la SSML di Mantova, a chi non è residente o domiciliato in Lombardia il costo del Master può essere parzialmente o interamente finanziato con formula Prestitempo di Deutsche Bank. Per informazioni contattare la dott.ssa Arianna Riva tel. 02 87388760, e-mail master.mn@unicollegessml.it

5 - RESPONSABILE DEL PROCEDIMENTO

1. Il responsabile del procedimento di cui al presente bando è la dott.ssa Arianna Riva, tel. 02 87388760, e-mail master.mn@unicollegessml.it
2. Le disposizioni del presente bando atte a garantire la trasparenza di tutte le fasi del procedimento e i criteri e le procedure per la nomina delle commissioni giudicatrici e dei responsabili del procedimento sono in attuazione della legge 7 agosto 1990, n. 241 e successive modificazioni.

6 - TRATTAMENTO DEI DATI PERSONALI

1. Ai sensi dell'articolo 13 del Decreto Legislativo 30 giugno 2003, n. 196, i dati personali forniti dai partecipanti al Corso per Master di cui all'articolo 1, sono raccolti presso la SSML di Mantova, con sede in via G. Rippa, 2.
2. Il trattamento dei suddetti dati avverrà esclusivamente per le finalità di cui al presente bando.
3. Il conferimento dei dati personali è obbligatorio ai fini della valutazione dei requisiti di partecipazione alla selezione, pena l'esclusione dalle procedure di selezione.
4. I dati personali forniti dai candidati possono essere comunicati dalla SSML di Mantova al Ministero per le finalità istituzionali proprie.
5. Ai candidati sono riconosciuti i diritti di cui all'articolo 7 del citato decreto legislativo n. 196/2003, in particolare il diritto di accesso ai dati che li riguardano e il diritto di ottenerne l'aggiornamento o la cancellazione se erronei, incompleti o raccolti in termini non conformi alla legge, nonché il diritto, per motivi legittimi, di opporsi al loro trattamento.
   Tali diritti possono essere fatti valere nei confronti della SSML di Mantova, con sede legale in via G. Rippa 2, 46100 Mantova, titolare del trattamento.

7 - DISPOSIZIONI FINALI

Per quanto non espressamente previsto dal presente bando si rimanda alla normativa e ai regolamenti vigenti presso la SSML di Mantova.

Mantova, 15/07/2016

Il Direttore Generale
F.to Prof. Simone Borile