Privacy & CyberSecurity

@PoliTO

Enrico Venuto
Politecnico di Torino

WORKSHOP GARR 2021

NET MAKERS

Politecnico di Torino

Mentimeter

9489 0567

Il Coordinatore per la Sicurezza Informatica di Ateneo

Con la "*Legge Privacy*" 196/2003 vengono introdotti e formalizzati le *Misure minime di sicurezza informatica* ed il *Documento Programmtatico della Sicurezza* (DPS).

Il Politecnico di Torino introduce due figure di nomina rettorale

- La figura del *Coordinatore per la Sicurezza Informatica di Ateneo* viene formalizzata nel 2006 con il *Regolamento di attuazione del Codice Privacy di Ateneo*, assieme a quella del *Coordinatore per il Trattamento dati di Ateneo*.
- Con il GDPR, la figura del *Coordinatore per il Trattamento Dati di Ateneo* evolve in quella del *DPO/RPD* (Responsabile Protezione Dati). Le *Misure minime* diventano *Misure adeguate al rischio* ed il *DPS* diventa il *Registro dei Trattamenti; Data Breach* sanzionato

Nomina del CISO

Il Titolare nomina un Coordinatore della Sicurezza Informatica di Ateneo (CISO) che è incaricato di svolgere, in piena autonomia e indipendenza, i seguenti compiti e funzioni:

a) *indirizzo, pianificazione, coordinamento e monitoraggio della sicurezza informatica relativamente ai dati, ai sistemi ed alle infrastrutture, anche in relazione al sistema pubblico di connettività, nel rispetto delle regole tecniche indicate nell'art 51 del D.lgs. 82/2005 [Lettera c) - Art. 17 - Comma 1 - D.Lgs. 82/2005 (CAD)]*

b) coordinamento con l'Ufficio per il digitale [RTD] e con la Commissione strategie per le Tecnologie dell'Informazione di Ateneo;

Nomina del CISO

c) supporto al Titolare del trattamento dei dati nella messa in atto delle misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio, per i diritti e le libertà delle persone, come previste dall'art. 32 del GDPR;

d) supporto al Titolare del trattamento in caso di violazione dei dati collaborando nelle attività previste all'art. 33 e 34 del GDPR conseguenti ad una violazione di dati;

e) collaborazione con il RPD di Ateneo per le tematiche riguardanti la protezione dei dati;

f) nomina degli *Amministratori di Sistema* di Ateneo in accordo con i Responsabili di Struttura e cura l'aggiornamento del relativo elenco.

Nomina del CISO

L'Ateneo si impegna a:

- Mettere a disposizione del CISO il supporto necessario al fine di consentire l'ottimale svolgimento dei compiti e delle funzioni assegnate anche attraverso la diretta collaborazione con *l'Unità di Sicurezza IT* dell'Area Information Technology
- Non rimuovere o penalizzare il CISO in ragione dell'adempimento dei compiti affidati nell'esercizio delle sue funzioni
- Garantire al CISO di esercitare le proprie funzioni in autonomia e indipendenza e in particolare, non assegnando allo stesso attività o compiti che risultino in contrasto o conflitto di interesse

Fra i suoi compiti

- Censisce i sistemi di sicurezza informatica di Ateneo
- Comunica le direttive sull'adozione delle misure di sicurezza informatica
- Coordina l'adozione delle misure di sicurezza informatica
- Promuove la formazione in materia di sicurezza del trattamento dei dati destinata al personale
- Ha accesso a tutte le risorse informatiche dell'Ateneo:
  - ai fini di azioni di monitoraggio sull'effettiva applicazione delle norme di sicurezza informatica e sulla privacy
  - ai fini di controlli occasionali a carattere preventivo volto alla difesa dei sistemi informatici o, a carattere successivo, volto all'accertamento delle responsabilità conseguenti alla commissione di illeciti

Definizioni
CISO – Chief Information Security Officer

- Il *Chief information security officer*, abbreviato in *CISO*, è, ove presente, il responsabile di massimo livello della sicurezza delle informazioni all'interno dell'organizzazione.
  [Profili professionali relativi alla sicurezza delle informazioni (UNI 11621-4)]
- Il CISO definisce la strategia per la gestione della sicurezza delle informazioni, coordinando i security manager, i fornitori o il personale specialistico per garantirne la continua e corretta attuazione nel tempo all'interno di un budget definito. A tal fine, vista la natura trasversale della sicurezza delle informazioni, si interfaccia anche con il top management dell'azienda e, secondo competenza, con tutte le figure di responsabilità aziendali.
  [AGID - Dizionario dei profili di competenza per le professioni ICT]

Conclusioni

Gestione del rapporto col RTD

La condizione di esistenza di un CISO nella PA è che le funzioni descritte alla Lettera c) - Comma 1 - Art. 17 - D.Lgs. 82/2005 (CAD) gli siano assegnate:

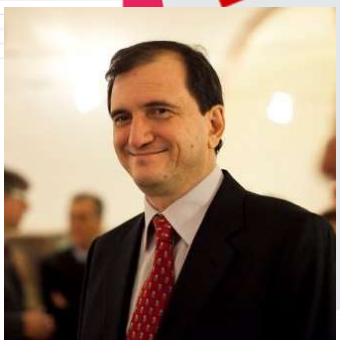
Indirizzo, pianificazione, coordinamento e monitoraggio della sicurezza informatica relativamente ai dati, ai sistemi ed alle infrastrutture

Designazione Ufficio per il digitale:

[...] di assegnare all'Area Information e Technology, i compiti attribuiti all'Ufficio per il digitale, previsti dall'art. 17 comma 1 del D.Lgs. 82/2005, con la sola esclusione del compito indicato alla lettera c) del medesimo provvedimento.

Privacy & CyberSecurity @PoliTO

THANK YOU



Enrico Venuto
venuto@polito.it

Politecnico di Torino

WORKSHOP GARR 2021

NET MAKERS

Mentimeter
9489 0567