ENTE ACCREDITATO DAL MINISTERO DELL'ISTRUZIONE, DELL' UNIVERSITÀ E DELLA RICERCA
PER LA FORMAZIONE DEL PERSONALE DELLA SCUOLA – DIRETTIVA 170/2016

Programma analitico d'esame

PRIVACY E SICUREZZA DEI DATI

Premessa

Il rapido evolversi delle tecnologie dell'informazione ha preteso una costante definizione di nuovi parametri di tutela della persona, anche in riferimento all'adattamento degli istituti giuridici già esistenti.

L'evoluzione tecnologica recente ha, dunque, innegabilmente modificato le modalità con cui i soggetti percepiscono la propria identità, l'immagine e le relazioni sociali, o più in generale, i vari aspetti della personalità.

La più recente capillare diffusione di internet, con i relativi strumenti di comunicazione, quali per esempio i social network, ha peraltro comportato l'ulteriore esigenza di coinvolgere anche la realtà virtuale nel modello di tutela tradizionalmente apprestato alla personalità.

La sfera della riservatezza si presta a essere la più vulnerata dai moderni mezzi di comunicazione e, pertanto, la definizione di privacy si arricchisce di nuovi significati partendo dal diritto a essere lasciati soli tipico del diciannovesimo secolo, sino alle più recenti istanze di tutela dei dati e dei mezzi tecnologici di protezione.

La prospettiva di lavoro tiene conto, pertanto, dell'evoluzione dei diritti della personalità generalmente intesi e declinati nella tutela della riservatezza, immagine, identità, manifestazione del pensiero e diritto d'autore, alla luce delle più moderne tesi di indagine.

Disclaimer

Certipass ha redatto il presente documento programmatico in base agli standard e ai riferimenti Comunitari vigenti in materia di competenze a carattere digitale. Il documento riporta le informazioni riguardanti il Programma di certificazione. Certipass non si assume alcuna responsabilità derivante dall'applicazione in ambito diverso dallo stesso, neanche da informazioni elaborate da terzi in base ai contenuti del presente Programma.

Certipass si riserva di aggiornare il presente documento a propria discrezione, in ogni momento e senza darne preavviso, pubblicando le modifiche effettuate. L'Utenza destinataria è tenuta ad acquisire in merito periodiche informazioni visitando le aree del sito dedicate al Programma.

Privacy e sicurezza dati

Il modulo intende fornire al candidato le necessarie competenze per occuparsi della gestione dei dati personali senza violare le normative sulla privacy e affrontare in modo adeguato le problematiche legate al tema della sicurezza informatica. Il punto di partenza è il concetto di privacy, con le regole in materia di protezione di dati personali, anche per i soggetti pubblici.

Le nuove tecnologie digitali pongono infatti numerosi interrogativi rispetto alla privacy, in quanto l'utilizzo dei servizi internet, della mail o degli acquisti su internet, e naturalmente anche i rapporti con la PA digitale richiedono continuamente il trattamento dei dati personali che non può essere lasciato ad un uso privo di limitazioni e procedimenti definiti e condivisi.

L'avvento del web 2.0 ha reso ancor più urgente la regolamentazione della privacy e le normative sulla sicurezza informatica in quanto ha reso ancora più diffusa e frequente la pratica della comunicazione sul web con la condivisione di file multimediali di ogni tipologia: dalle foto, ai video, ai messaggi testuali o audio.

Il candidato dovrà dimostrare la conoscenza dei seguenti argomenti:

- Privacy: definizione ed evoluzione
- Codice in materia di protezione dei dati personali
- I diritti dell'interessato
- Le regole in materia di protezione dei dati personali
- Le regole specifiche dei soggetti pubblici
- Privacy e diritto di accesso
- Le misure di sicurezza
- Il disaster recovery

ARGOMENTO 1

LA PROTEZIONE DEI DATI IN INTERNET: ASPETTI GIURIDICI

e-Competence Framework | e-CF intermediate

Come è noto il 1° gennaio 2004 è entrato in vigore il Codice per la protezione dei dati personali che ha notevolmente irrobustito il sistema della protezione dei dati personali, ormai solidamente collocata nel quadro dei diritti fondamentali. Difatti viene riconosciuto nel nostro ordinamento l'autonomo diritto alla protezione dei dati personali in armonia con quanto già previsto nella Carta dei diritti fondamentali dell'Unione europea e nel progetto di Costituzione europea.

TESTING

	Conoscenza teorica/Knowledge (K) *Il Candidato conosce, è informato, ha familiarità con…*		Competenze pratiche / Skills (S) *Il Candidato è capace di*
K1.1	**Il concetto di privacy**	**S1.1**	**Definire il concetto di privacy**
K1.2	**Regole generali in materia di protezione di dati personali**	**S1.2**	**Conoscere le regole generali in materia di protezione di dati personali, contenute nel Capo I del Titolo I del Codice per la protezione dei dati personali**
K1.3	**Regole per i soggetti pubblici**	**S1.3**	**Conoscere le regole a cui devono attenersi i soggetti pubblici**
K1.4	**La protezione dei dati nel Regolamento (UE) 2016/679**	**S1.4**	**Conoscere la nuova definizione di dato personale proposta dal legislatore europeo e i principi di liceità, correttezza e trasparenza**
K1.5	**La tutela dei dati in internet**	**S1.5**	**Conoscere il diritto al risarcimento del danno da lesione del diritto alla riservatezza**

ARGOMENTO 2

LE MISURE DI SICUREZZA INFORMATICA

e-Competence Framework | e-CF intermediate

Le reti sono sistemi che consentono di conservare, elaborare e veicolare i dati. Si compongono di elementi trasmissivi (cablaggio, collegamenti senza filo, satelliti, router, gateway, commutatori, ecc.) e di servizi di supporto (sistema dei nomi di dominio — DNS con relativo roote server, servizio di identificazione della linea chiamate, servizi di autenticazione, ecc.). Le reti sono collegate a svariati applicativi (sistemi di consegna di posta elettronica, browser, ecc.) e apparati terminali (apparecchio telefonico, computer host, PC, telefono mobile, palmare, elettrodomestici, macchinari industriali, ecc.)» . La rete è caratterizzata dai seguenti elementi: (1) disponibilità; (2) autenticazione; (3) integrità; (4) riservatezza. In questa sezione si vedranno le misure di sicurezza applicabili.

TESTING

	Conoscenza teorica/Knowledge (K) *Il Candidato conosce, è informato, ha familiarità con…*		Competenze pratiche / Skills (S) *Il Candidato è capace di*
K2.1	**Le misure di sicurezza informatica: profili generali**	**S2.1**	**Definire il concetto di rete, le sue caratteristiche e il profilo generale delle misure di sicurezza**
K2.2	**Le misure minime di sicurezza**	**S2.2**	**Conoscere le misure minime di sicurezza**
K2.3	**Il trattamento dei dati mediante l'ausilio di sistemi elettronici**	**S2.3**	**Conoscere le misure per il trattamento dei dati secondo gli obblighi attesi dal Codice della Privacy**
K2.4	**Misure di sicurezza in materia di trattamento dei dati sensibili e giudiziari**	**S2.4**	**Conoscere le misure di sicurezza intese come risvolto dinamico del concetto giuridico di sicurezza**
K2.5	**Le violazioni delle misure di sicurezza informatica**	**S2.5**	**Definire lo standard internazionale di valutazione della sicurezza informatica: confidenzialità, integrità, disponibilità. Conoscere le misure idonee per evitare la violazione delle misure di sicurezza**
K2.6	**Il disaster recovery**	**S2.6**	**Definire il piano di continuità operativa e il disaster recovery. Conoscere le procedure tecniche e organizzative relative**

ARGOMENTO 3

LA PROTEZIONE DEI DATI IN INTERNET: ASPETTI TECNICI

e-Competence Framework | e-CF intermediate

L'IT Security comprende tutte quelle attività finalizzate alla protezione dei dati attraverso misure di carattere tecnico-organizzativo e funzionali tese ad assicurare la conservazione e la trasmissione integra dei dati, la confidenzialità, l'autenticazione, la disponibilità e la funzionalità corretta di hardware e software.

TESTING

	Conoscenza teorica/Knowledge (K) *Il Candidato conosce, è informato, ha familiarità con…*		Competenze pratiche / Skills (S) *Il Candidato è capace di*
K3.1	**Tecniche di protezione dei dati** K3.1.1 Lo storage. K3.1.2 Il backup dei dati e il loro ripristino.	**S3.1**	**Definire lo scopo delle tecniche di protezione dei dati e identificare le più comuni** S3.1.1 Sapere come salvare in modo sicuro i dati scambiati e su quali dispositivi. S3.1.2 Saper realizzare un backup dei dati e il ripristino.
K3.2	**IT Security** K3.2.1 I diversi livelli di protezione. K3.2.2 Gli attacchi informatici. K3.2.3 Gli attacchi login. K3.2.4 Gli strumenti di difesa.	**S3.2**	**Definire l'IT Security e il suo funzionamento** S3.2.1 Conoscere le minacce, le misure di protezione attive e le misure di protezione passive. S3.2.2 Riconoscere gli attacchi informatici. S3.2.3 Conoscere e definire lo sniffing, lo spoofing, il thiefing, il keylogger, il phishing. S3.2.4 Conoscere i principali strumenti di difesa.

www eipass com

info@eipass.com

NUMERO VERDE
800.088.331