**ABSTRACT**

**CORSO DI FORMAZIONE ON-LINE**

**LA SICUREZZA INFORMATICA A SCUOLA: LE MISURE ADEGUATE PREVISTE DAL GDPR**

Quella della **sicurezza informatica** nella pubblica amministrazione, e in particolare nella scuola italiana, è una storia che parte da lontano. Purtroppo, i diversi piani avviati non hanno ancora risolto alcuna questione **cruciale**, dalla governance ai controlli, fino alla **formazione del personale**, il tutto in un contesto in cui **la quantità e la qualità della minaccia cibernetica è in continuo aumento, così comela digitalizzazione e l’offerta di servizi in rete**.

Con l’entrata in vigore del GDPR, il trattamento dei dati personali in ambito scolastico, inoltre, ha evidenziato una serie di problematiche su più livelli. Da quelle relative alla struttura tecnologica e al modello organizzativo, a quelle legate alla **consapevolezza dell’adozione delle misure di sicurezza informatica nell’utilizzo degli strumenti digitali**.

Il GDPR impone la valutazione riguardante gli aspetti della riservatezza dei dati e dell’integrità e disponibilità degli stessi.Per raggiungere questo ambizioso obiettivo, nel rispetto del principio di **accountabilty**, è inevitabile prevedere delle misure **adeguate di sicurezza, tecniche e organizzative**.

In ambito scolastico, è proprio l’origine del dato personale a portare con sé **rischi elevati** in quanto, quasi sempre, **connesso a minori**. Il trattamento, inoltre, opera su dati che rivelano l’origine etnica e religiosa e dati sanitari.

Le prassi che la Scuola, costantemente sollecitata da numerosi gravami amministrativi e organizzativi, ha sviluppato dopo l’avvento del GDPR evidenziano numerose **non conformità**.

Un esempio è **l’utilizzo improprio**, per attività istituzionali, **degli account email personali**, forieri di newsletter e spam. Tale prassi, parecchio diffusa, espone i dati della scuola a **molteplici rischi**, quali distruzioni, viralizzazioni e potenziali divulgazioni o sottrazioni di dati, in caso di errore umano o di truffe informatiche (phishing).

Tutte le attività scolastiche vengono svolte attraverso sistemi informatici che elaborano e conservano i dati relativi a studenti e loro familiari, personale dipendente, fornitori.

Per tale motivo **il tema della sicurezza informatica riveste un’importanza fondamentale e strategica**. Ciò è ancor più evidente se si considera il costante **aumento delle violazioni** (più o meno rilevanti) ai sistemi informatici o le numerose perdite di dati e di informazioni dovute a **comportamenti negligenti o imprudenti** dei dipendenti pubblici o, ancora, a **malfunzionamenti** dei sistemi informatici o telematici.

Il MIUR rileva l’esigenza di una **rinnovata responsabilizzazione degli attori principali del trattamento dei dati personali nella scuola**, chiedendo di prendere effettiva cognizione della necessità di attivarsi concretamente per garantire una **efficace protezione dei dati personali** che non sia più limitata a un asettico recepimento di una serie di obblighi preconfezionati di sicurezza.

La **sicurezza informatica** scaturisce prima di tutto da una **corretta percezione del personale** e, in generale, da tutti coloro che utilizzano i servizi tecnologici messi a disposizione dalla scuola.

È inutile definire policy di sicurezza IT se poi un operatore le disattende eseguendo un allegato di posta elettronica o aprendo un improbabile file, in quanto nessuno lo ha formato.

Ogni policy va esposta, **facendo comprendere agli interessati che sono parte attiva** del processo di messa in sicurezza dei dati della scuola.È necessario **farsi carico di formare e chiarire** cosa sono, ad esempio, le attività di phishing, cosa possono provocare e come evitarle.

Tuttavia, le policy devono anche riflettere la realtà dell’istituto e vanno quindi **create e modulate sulla reale contingenza della scuola,** evitando il rischio opposto cioè quello di ingessare la stessa con pratiche o procedure inutili ed ininfluenti sul piano della **sicurezza informatica**.

La finalità del corso si sostanzia **nell’acquisizione ragionata, consapevole e responsabile, da parte del personale scolastico, delle tecniche, strategie e procedure dei fondamenti di sicurezza informatica.**

**Struttura**

Il percorso si svilupperà secondo un approccio **Webinar della durata di 25**oreOgni concetto e ogni tecnica appresa verrà immediatamente applicata in situazione.

**Metodologia di lavoro**

* Relazioni di approfondimento sui temi del corso.
* Training attivo attraverso esercitazioni e simulazioni.
* Analisi di casi e ricerca di soluzioni attraverso esercizi di problemsolving cooperativo.

**Di seguito il dettaglio del percorso di formazione**

**Modulo 1 - Privacy e Sicurezza Informatica nella scuola**

* Il GDPR e le misure di sicurezza informatica a protezione della Privacy
* I principi della protezione dei dati personali e le misure di sicurezza informatica (minime) adeguate
* Il panorama della sicurezza informatica in Italia e l’obbligo, per la pubblica amministrazione, di consultare il Cert-PA
* L’analisi dei rischi dei trattamenti di dati personali nella Scuola.

**Modulo 2 - La check-list della sicurezza IT**

* L’obbligatorietà del regolamento per la sicurezza informatica nelle scuole
* L’inventario delle dotazioni tecnologiche e dei software
* Minacce e attacchi e relative procedure per la sicurezza informatica sui PC e su Internet.
* La gestione dei sistemi informativi scolastici.

**Modulo 3 - Valutazione e correzione della vulnerabilità**

* Indicazioni per il ripristino istantaneo dei PC dedicati all’attività amministrativa e alla attività didattica
* Come rilevare la presenza di software non licenziato e/o non autorizzato
* La continuità operativa: obbligo e opportunità per la pubblica amministrazione
* Cosa fare in caso di Data Breach (Art. 33 e 34 del GDRP – Regolamento UE Privacy 679/2016)

**Modulo 4 - Esempi di soluzioni pratiche adottate, con successo, da parte di altre scuole**

**Durata complessiva di svolgimento dell'attività**

20 ore in attività asincrona, complessive per le videolezioni, la presentazione di materiali con casi studio, le esercitazioni personali.