ECDL IT Security: ecco come ottenere la certificazione

sicurezza.net
21 Maggio 2021

ECDL IT Security è una certificazione che attesta le conoscenze sulle minacce **cyber** e sulla gestione dei **dati**. È, inoltre, sfruttabile per alcuni concorsi.

La certificazione ECDL IT Security rappresenta in un mondo sempre più connesso e, di conseguenza, a rischio di infiltrazioni da parte di terzi all'interno dei dati personali, una valida **attestazione** delle conoscenze per far fronte a tali minacce.

Non solo testimonia la capacità di gestire pericolo cyber ma è, inoltre, spendibile in alcuni **concorsi** e, in generale, nel mondo del lavoro.

L'attestato, infatti, fornisce agli utenti tutte le competenze necessarie per identificare le minacce alla sicurezza informatica quali, ad esempio, **virus**, **phishing** e **hacker**, al fine di poter porre rimedio.

L'ECDL fa riferimento in Italia all'**AICA**, con la quale si definisce l'Associazione Italiana per l'Informatica e il Calcolo Automatico, ente che gestisce le certificazioni tutte e i test center, vale a dire i luoghi accreditati per lo svolgimento degli esami da parte dei candidati.

Il programma ECDL, conosciuto anche con il nome di **ICDL**, International Certification of Digital Literacy, si articola in una serie di certificazioni volte a dimostrare le conoscenze informatiche degli utenti che ne fanno richiesta.

Si strutturano, infatti, da un livello base fino a uno avanzato.

L'attestazione in esame, appartenendo a un livello superiore o specialistico, può essere anche conseguita come **certificato singolo**.

Come è strutturata la certificazione ECDL IT Security

La certificazione ECDL IT Security si riferisce, come accennato, a un'utenza che usufruisce ampiamente dei **sistemi informatici** e che, dunque, è bene conosca i pericoli in cui può incappare in termini di sicurezza.

L'ente, infatti, richiede al candidato la conoscenza dei concetti relativi alla sicurezza informatica, le modalità attraverso cui proteggere i dati in suo possesso nonché come identificare le minacce del web e le tipologie di **malware**.

Per comprendere l'utilità che risiede nel conseguimento di tale certificazione, bisogna analizzare le sezioni di cui si compone.

In primo luogo è bene sottolineare che le unità sono **sette** e ognuna di esse è caratterizzata da temi specifici.

Prima sezione della certificazione

La prima sezione si focalizza su tutti i temi di sicurezza e si ramifica in quattro aree.

Al principio si trattano temi di **hacking** e, dunque, di tutto ciò che riguarda le minacce ai dati personali.

Successivamente, si analizzano i contenuti di integrità e disponibilità dati e la necessità di proteggere questi ultimi siano loro di natura personale o aziendale.

Ancora, i temi della prima unità si concentrano sulla **sicurezza personale** e, in particolare, sul furto di identità e sul phishing nonché sulla tutela dei file al fine di far acquisire capacità tecniche quali la cifratura dei file stessi.

Seconda sezione

La seconda sezione, invece, mette a fuoco i **malware**, mediante l'analisi delle sue tipologie come, ad esempio, il **ransomware** o il **keylogger**, per comprenderne il funzionamento.

Una volta appreso come riconoscerli, si procede alle tecniche di difesa e dunque si effettuerà un'analisi degli **antivirus**, la messa in quarantena di file ritenuti sospetti e i metodi per risolvere un attacco con risorse fruibili online.

Terza sezione

La terza sezione è incentrata sulla **sicurezza in rete** mediante due metodi.

Da una parte l'analisi di reti e connessioni per apprendere le implicazioni di sicurezza per le reti **LAN**, VPN e Wan, dall'altra quella sulle reti **wireless**. Si giunge, quindi, a comprendere come utilizzare un **firewall** personale nonché come attivare un hotspot personale.

Quarta sezione

Altra unità è focalizzata sul **controllo di accesso** per rendere all'utente i metodi efficaci sia per evitare accessi non autorizzati ai dati che per la gestione delle password. Si comprendono, infatti, i metodi per impostare password di livello.

Quinta sezione

Nella quinta sezione dell'ECDL IT Security i discenti apprenderanno come sfruttare in modo corretto il **web**.

Il tema riguarderà le impostazioni del browser e la navigazione sicura. Alcuni esempio sono la cancellazione della cronologia e le modalità attraverso cui confermare l'autenticità di un sito.

Sesta sezione

La penultima unità è incentrata, invece, sulla **comunicazione**.

I quattro temi di cui si compone sono relativi alle email, alla messaggistica istantanea, alle reti sociali e ai dispositivi mobili.

Per ognuno di essi sono illustrati i processi per identificare minacce quali, ad esempio nel primo caso, il **phishing**.

Il secondo caso, invece, è volto a insegnare la **vulnerabilità** della messaggistica istantanea e del Voice over IP, rappresentata da malware o accessi da backdoor.

Nel terzo caso l'obiettivo è far apprendere l'importanza della non trasmissione di informazioni personali su tali siti e sulla gestione dei propri account, sviscerando le minacce rappresentate da link malevoli in cui ci si può imbattere.

Settima sezione

L'ultima sezione dell'ECDL IT Security, infine, è incentrata sulla **gestione sicura dei dati**.

Gli utenti scoprono come effettuare copie di sicurezza di dati e come salvaguardare la sicurezza fisica del pc e/o dei dispositivi mobili.

Inoltre, l'unità si chiude insegnando a distruggere i dati definitivamente e il motivo per cui compiere tale operazione è fondamentale.

Come si ottiene la certificazione ECDL IT Security

In precedenza si è fatto riferimento all'AICA. È, infatti, sul sito di questo ente che si deve sottoscrivere la **domanda** di certificazione.

Gli utenti interessati possono studiare individualmente i manuali di riferimento per avvicinarsi al giorno dell'esame.

Quest'ultimo si potrà effettuare in una delle sedi d'esame accreditate, dove gli iscritti acquisteranno una **Skills Card**, si registreranno alla prova e una volta superata faranno richiesta di certificazione rilasciata, appunto, dall'AICA.

L'ente, infine, mette a disposizione per gli interessati dei "**sample test**" da completare in modo da concedere agli esaminandi una panoramica generale dell'esame che andranno ad affrontare prima di effettuarlo ufficialmente.