Manuale ECDL Full Standard

Modulo Computer Essentials

Sicurezza e benessere

Capitolo 10 – Sicurezza e benessere

Riferimento Syllabus 6.1.1	*Riconoscere politiche corrette per le password quali crearle di lunghezza adeguata con un'adeguata combinazione di caratteri, evitare di condividerle, modificarle con regolarità*
Riferimento Syllabus 6.1.2	*Definire il termine firewall e identificarne gli scopi*
Riferimento Syllabus 6.1.3	*Comprendere lo scopo di creare con regolarità copie di sicurezza remote dei dati*
Riferimento Syllabus 6.1.4	*Comprendere l'importanza di aggiornare regolarmente i diversi tipi di software quali antivirus, applicazioni, sistema operativo*
Riferimento Syllabus 6.2.1	*Definire il termine "malware". Identificare diversi tipi di malware, quali virus, worm, Trojan, spyware*
Riferimento Syllabus 6.2.2	*Sapere come un malware può infettare un computer o un dispositivo*
Riferimento Syllabus 6.2.3	*Usare un software antivirus per eseguire una scansione in un computer*
Riferimento Syllabus 6.3.1	*Sapere quali sono i principali modi per assicurare il benessere di un utente durante l'uso di un computer o di un dispositivo, quali effettuare pause regolari, assicurare una corretta illuminazione e postura*
Riferimento Syllabus 6.3.2	*Conoscere le opzioni di risparmio energetico che si applicano ai computer e ai dispositivi elettronici: spegnimento, impostazione dello spegnimento automatico, dell'illuminazione dello schermo, della modalità di sospensione*
Riferimento Syllabus 6.3.3	*Sapere che i computer, i dispositivi elettronici, le batterie, la carta, le cartucce e i toner delle stampanti dovrebbero essere riciclati*
Riferimento Syllabus 6.3.4	*Identificare alcune delle opzioni disponibili per migliorare l'accessibilità, quali software di riconoscimento vocale, screen reader, zoom, tastiera su schermo, contrasto elevato.*
Contenuti della lezione	Username e password; Politiche corrette per le password; Il firewall; Copia di sicurezza; L'importanza di aggiornare con regolarità; Aggiornamento dell'antivirus; I malware; I diversi tipi di malware; Come agisce un malware; I pericoli della rete locale; I pericoli da internet; I pericoli della posta elettronica; Antivirus e scansione; Programmi antivirus; Usare un antivirus per eseguire la scansione; L'ergonomia; La giusta illuminazione; La corretta postura; Le opzioni di risparmio energetico; Il riciclo di cartucce, carta e dispositivi elettronici; Migliorare l'accessibilità al computer.

Username e password

La politica della sicurezza in ambito informatico interessa vari aspetti: dalla collocazione fisica di computer e archivi in luoghi in cui sia possibile evitare danneggiamenti fisici, al controllo degli accessi per evitare intrusioni.

Tale controllo è effettuato dai sistemi operativi, mediante assegnazione sia di **user id** e **password** individuali da assegnare al momento dell'accesso al sistema, sia di definizione di privilegi.

Politiche corrette per le password

Per garantire la sicurezza, una password deve rispondere ad una serie di requisiti:

- non deve essere riconducibile ad un soggetto fisico;
- deve avere una lunghezza minima di 8 caratteri;
- non deve essere una parola del dizionario o il nome di un parente o amico;
- deve contenere caratteri maiuscoli e minuscoli, caratteri speciali e numeri.

È bene, inoltre, che abbia una scadenza periodica e non venga mai condivisa con nessuno.

APPROFONDIMENTO

Per prevenire il furto di dati, soprattutto in luoghi pubblici ma anche in ambiente aziendale o scolastico, è importante conoscere e mantenere alcune buone consuetudini:

- evitare di accedere al computer senza autenticazione, ma impostare il proprio account in modo che all'accesso venga richiesto il nome utente e la password
- adottare una password anche per l'accesso e lo sblocco del proprio smartphone
- quando si smette di utilizzare il computer o un servizio internet che richiede la connessione, effettuare la disconnessione, per evitare che un malintenzionato possa utilizzarla al vostro posto
- quando ci si allontana momentaneamente dal computer che si sta utilizzando, bloccare l'accesso usando il comando **Blocca** del menu **Start** o premere la combinazione di tasti [**Ctrl+Alt+Canc**] e selezionare **Blocca computer**. Ciò farà comparire la finestra di logon che richiede la digitazione della password per riattivarlo. Il metodo più veloce è però l'utilizzo della combinazione di tasti [**Win+L**].

Il firewall

Un **firewall** (traducibile con il termine di "muro tagliafuoco") è un componente di difesa frapposto tra una rete privata e Internet.
La sua presenza consente di dividere la rete in due parti: una esterna, la **WAN**, che comprende l'intera Internet, l'altra interna rappresentata dalla **LAN**.
In alcuni casi è possibile che nasca l'esigenza di creare una terza zona detta **DMZ**, acronimo di "De Militarized Zone" cioè zona demilitarizzata.
Questo segmento di LAN è atto a contenere quei sistemi che devono essere isolati dalla rete interna ma devono poter essere accessibili da Internet; tipicamente si tratta dei server web.

APPROFONDIMENTO

Il firewall può essere implementato su un server dedicato o su un apparato di rete, oppure può essere un software in esecuzione su un computer. Indipendentemente da come è realizzato, il suo compito è quello di monitorare il traffico di rete e filtrarlo in base ad opportune regole che garantiscano la sicurezza di tutti i dati in entrata e in uscita, da e verso la rete o il computer, bloccando ciò che si ritiene pericoloso o indesiderato.

Un firewall, quindi, riduce il rischio di accessi indesiderati, al proprio computer o alla propria rete locale provenienti dall'esterno, tipicamente da Internet.

Copie di sicurezza

Sono molteplici le cause per cui i dati possono andare persi: cattiva gestione, furto, danneggiamento fisico del computer.

È bene quindi tutelarsi dalla perdita accidentale delle informazioni mediante **copie di backup** che permettono una ricostruzione degli archivi.
Ogni evento distruttivo prevede una specifica **modalità di backup** dei dati.

Per proteggersi da malfunzionamenti hardware o da errori di utilizzo è sufficiente fare una copia dei dati importanti mentre, per proteggersi da infezioni da virus o da furti è necessario utilizzare supporti di **memoria removibile** e conservare le copie di backup in un luogo sicuro.

La frequenza con la quale effettuare le copie di backup dipende dalla natura dei dati e dall'entità degli aggiornamenti effettuati.

APPROFONDIMENTO

Le copie di sicurezza possono essere fatta su supporto magnetico (nastro, disco rigido esterno), ottico (dvd, blu-ray) oppure, ed oggi è sempre più diffuso, direttamente su un server remoto via internet.

L'importanza di aggiornare con regolarità

Tutti i programmi informatici possono contenere dei difetti, in gergo chiamati" **bug**".
È fisiologico che con l'aumentare delle righe di codice del programma cresca anche la probabilità di inserire un errore. Ed i sistemi operativi, come dimostra la realtà quotidiana, non sono esenti da problemi di questo genere.
Per questo esistono gli "**update**": piccoli o grandi aggiornamenti che le case sviluppatrici di software rilasciano per risolvere i problemi individuati dagli utenti.

Windows ad esempio dispone del programma **Windows update** che con cadenza generalmente mensile scarica e installa tutti gli aggiornamenti del sistema operativo e delle applicazioni Microsoft.

Come mai gli aggiornamenti assumono così tanta importanza? Se un software ha un bug, non funziona al suo meglio. Un aggiornamento, in gergo detto **patch**, serve proprio a correggere un malfunzionamento del programma in termini di funzionalità, prestazioni o sicurezza.

APPROFONDIMENTO

Spesso si sottovaluta il pericolo di un bug in rapporto alla sicurezza. Sono molti i casi accertati in cui un hacker ha saputo sfruttare il difetto per introdursi nel sistema preso di mira. Per questa ragione si può notare che la maggior parte degli aggiornamenti di Windows è rilasciata per eliminare una qualche vulnerabilità alla sicurezza.

Aggiornamento dell'antivirus

Tra i software da aggiornare non va dimenticato **l'antivirus**, anche se qui l'elemento da aggiornare è raramente l'antivirus stesso ma è costituito dalle definizioni dei virus che, purtroppo, cambiano ogni giorno.

Sebbene la maggior parte del software antivirus sia progettata per eseguire l'aggiornamento in modo automatico, è possibile effettuare l'aggiornamento anche in modo manuale.

I malware

Il termine "virus informatico" è spesso usato in modo improprio. Quando infatti ci si vuol riferire genericamente ad un qualsiasi software in grado di causare danni ad un computer, si dovrebbe utilizzare il termine "**Malware**".

Questa parola deriva dalla contrazione delle parole inglesi "**MALicious softWARE**" e ha dunque il significato letterale di "programma malvagio" ma traducibile in italiano con il termine "codice maligno".

I diversi tipi di malware

Esistono vari tipi di malware. Di seguito una breve descrizione dei più conosciuti.

- **virus**, è un software in grado di infettare dei file eseguibili in modo da riprodursi facendo copie di se stesso, e di diffondersi tramite Internet oppure supporti removibili

- **worm**, è simile ad un virus, ma a differenza di questo non necessita di legarsi ad altri eseguibili per diffondersi e replicarsi. Tipicamente, modifica il computer che infetta in modo da venire eseguito ogni volta che si avvia la macchina e rimanere attivo finché non si spegne il computer o non si arresta il processo corrispondente.

- **trojan** (o cavallo di troia), deve il suo nome al fatto che le sue funzionalità sono nascoste all'interno di un programma apparentemente utile; e dunque l'utente stesso che installando ed eseguendo un certo programma, inconsapevolmente, installa ed esegue anche il codice trojan nascosto al suo interno

- **spyware** (o programma spia), è un software che raccoglie informazioni riguardanti l'attività online di un utente senza il suo consenso, trasmettendole tramite Internet ad un'organizzazione che le utilizzerà per trarne profitto. Le informazioni carpite possono andare dalle abitudini di navigazione fino alle password e alle chiavi crittografiche di un utente

APPROFONDIMENTO

L'elenco dei malware, purtroppo, è molto più lungo! Dialer, hijacker, rootkit, keylogger, scareware, rabbit, adware, ed altri ancora ne sono parte integrante.

Come agisce un malware

Per diffondersi, un virus o altri malware hanno bisogno di "viaggiare" da un computer all'altro e questo può avvenire sia tramite un supporto removibile (ZIP, DVD, CD-ROM, chiavetta USB) sia attraverso una rete, (locale o Internet).

Dato che i virus possono infettare sia i programmi eseguibili, sia i normali documenti sia il settore di avvio, appare evidente che è sufficiente eseguire il programma infetto o aprire un documento infetto per propagare l'infezione sul disco rigido o su altri supporti collegati al computer.

Non va poi dimenticato che con la diffusione dei software di messaggistica istantanea, anche questo è diventato un mezzo di diffusione dei virus

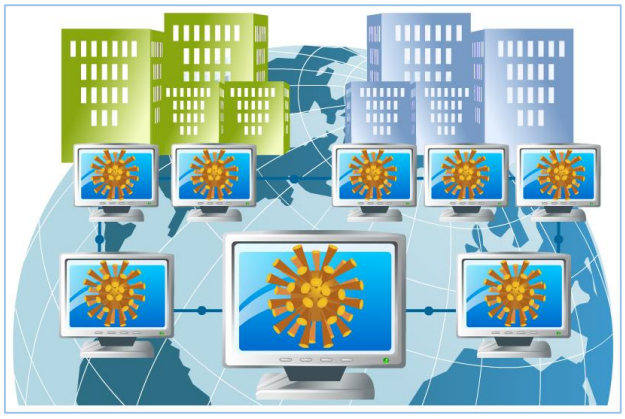
APPROFONDIMENTO

La diffusione di malware attraverso supporti removibili, al cui elenco classico è opportuno aggiungere anche schede di memoria e lettori mp3, è stato per lungo tempo favorito da una caratteristica di Windows tutto sommato piacevole, la funzionalità "autorun". Sfortunatamente, se viene eseguito automaticamente il file di avvio di un supporto infetto, si potrebbe restare contagiati senza alcuna possibilità d'intervento. Per questa ragione, Windows 7 e 8 disabilitano questa possibilità per impostazione predefinita lasciando all'utente la possibilità di attivarla in modo selettivo.

I pericoli della rete locale

Anche le reti locali costituiscono un elemento che può fungere da propagatore del virus, specie se queste collegano tra loro molti computer in posti diversi.

Un virus può colpire il server della rete e propagarsi sui client che eseguono i programmi infetti del server o che aprono documenti condivisi infetti.



I pericoli da Internet

Per quanto riguarda Internet non esiste il pericolo diretto di infezione virale, tuttavia può esistere un più generico problema di sicurezza legato al fatto che il programma di navigazione non solo legge dei dati ma esegue del codice dannoso per il computer.

Di norma il pericolo giunge invece dai file scaricati o eseguiti direttamente dal link della pagina visitata.

I pericoli della posta elettronica

Diverso è il discorso che riguarda la posta elettronica. In generale, la posta che giunge via Internet non può trasmettere virus informatici.

E' però necessario **distinguere tra posta e allegati**.

Infatti, ad un messaggio di posta è possibile allegare qualsiasi cosa, come un programma o un documento contente un virus informatico. Se l'utente decide di eseguire il programma accluso o aprire il documento si espone al rischio di contrarre il virus.

Antivirus e scansione

Per proteggere il computer dai virus e da altre minacce è necessario adottare misure adeguate e costanti, come l'installazione e l'aggiornamento di un **programma antivirus**.

Un programma antivirus è un programma molto complesso in grado di assolvere una moltitudine di compiti quali la rilevazione di comportamenti anomali del sistema, la scansione dei file critici e la rilevazione di virus sconosciuti.

La **scansione antivirus** è un'operazione manuale o pianificata con la quale si cerca la presenza di virus su un file, una cartella o un'unità.
Tale operazione dovrebbe essere eseguita su base periodica o comunque con una certa regolarità e in ogni caso ogni qual volta si sospetti la presenza di un virus.

APPROFONDIMENTO

Esistono altre misure, che è consigliato adottare, per proteggere il computer dai virus:

Mantenere Windows aggiornato. Microsoft rilascia periodicamente speciali aggiornamenti per la sicurezza che possono risultare utili per proteggere il computer. Questi aggiornamenti consentono di prevenire la diffusione di virus e attacchi da altri computer, chiudendo le possibili falle.

È pertanto necessario assicurarsi che Windows riceva questi aggiornamenti, attivando gli aggiornamenti automatici di Windows.

Utilizzare un firewall. *Windows Firewall*, o altri programmi analoghi, avvisano l'utente in caso di attività sospette se un virus o un worm tenta di connettersi al computer. Possono inoltre impedire il tentativo di virus, work e pirati informatici di scaricare programmi potenzialmente pericolosi sul computer.

Programmi antivirus

Sul mercato esistono molti programmi antivirus, gratuiti e a pagamento. Esempi gratuiti sono **Avast**, **Avira**, **AVG**, **Bitdefender**, **Panda** e molti altri.

Per eseguire la scansione del computer basta lanciarla dalla sua console principale o dall'icona del programma sempre presente nell'area di notifica.
Ad esempio, in AVG, il menu "**Scansione**" offre tre opzioni: **intero computer**, **file e cartelle** e **antirootkit**.
Dopo la scansione una finestra di riepilogo mostra i risultati dell'analisi.

APPROFONDIMENTO

Utilizzando la console del programma si possono controllare molti più aspetti delle sue funzionalità e impostare molte opzioni stabilendo con precisione il livello di scansione desiderato. Ad esempio si può impostare l'analisi degli archivi compressi, dei cookie di rilevamento, dei file senza estensione, ecc.

Usare un antivirus per eseguire la scansione

La scansione può essere avviata da una finestra del file system, utilizzando il menu contestuale e quindi scegliendo il comando Controlla seguito dal nome dell'oggetto su cui si effettua la scansione.

La rilevazione di un virus durante una scansione manuale è di norma totalmente automatico e non richiede l'intervento dell'utente.

A fine scansione la finestra di riepilogo presenterà il numero di virus trovati ed eliminati secondo le varie possibilità.

In presenza di un virus non rimovibile si ha sempre l'opzione di porlo in quarantena, cioè nello speciale stato di isolamento dove non può nuocere.

L'ergonomia

Per ergonomia si intende una disciplina che si occupa dell'attività umana in relazione alle condizioni ambientali, strumentali e organizzative in cui questa si svolge e che mira, appunto, alla salute e al benessere di chi lavora.

La giusta illuminazione

In merito all'illuminazione del posto di lavoro, devono essere rispettate le seguenti regole:

- Evitare l'illuminazione diretta del monitor da parte delle sorgenti luminose.
- Servirsi di lampade, a incandescenza o a fluorescenza, dotate di diffusori, per integrare l'illuminazione naturale.
- Privilegiare arredi con superfici opache e chiare, per evitare riflessi.
- Porre lo schermo del computer in posizione laterale rispetto alle pareti con finestre e, nel caso in cui una finestra sia di fronte, fare in modo che questa venga schermata con tende.

La corretta postura

Sono riportate di seguito alcune semplici regole relative alla posizione corretta da assumente quando si lavora a computer.

Monitor

Per evitare dolori al collo è bene posizionare il video in modo che lo sguardo sia inclinato di 20-30 gradi verso il basso.

Tastiera

La tastiera deve essere leggermente inclinata, utilizzando i piedini.

Mouse

Il mouse deve essere facilmente raggiungibile e il polso deve poter poggiare sulla superficie, in modo da evitare sforzi dannosi.

Sedia

La sedia deve sostenere bene la colonna vertebrale; a questo scopo può essere utile munirsi di un cuscinetto lombare.

Appoggio per i piedi

Gli appoggi per i piedi possono dare giovamento a chi non riesce a mantenere i 90 gradi di flessione delle ginocchia e delle caviglie.

APPROFONDIMENTO

Un ambiente ergonomico è indispensabile, ma nonostante questo riduca lo stress e il disagio, è importante anche un buon comportamento attivo da parte dell'utente, che riduca ai minimi termini i disagi:

- Mini pause a intervalli regolari: fare un mini stretch, alzandosi, muovendosi, facendo un'altra cosa, come telefonare. Ciò, anche se non rappresenta una vera pausa, permette di interrompere l'uso degli stessi muscoli
- Relax: ogni 30-60 minuti fare una vera pausa, durante la quale muoversi e distrarsi. Bere qualcosa, e riposare le zone del corpo più stanche.

Le opzioni di risparmio energetico

È evidente quanto sia importante prestare attenzione ai problemi energetici e operare, anche nelle attività quotidiane, nel rispetto delle regole che riducono lo spreco.

Considerando che un computer desktop in piena attività con monitor, stampante e accessori ha un consumo energetico che può arrivare a 500Watt/h, è bene spegnere il computer quando non viene utilizzato e verificare che anche lo schermo sia spento.

Tutti i computer e le periferiche attuali dispongono di sistemi di risparmio energetico che, nel caso dei computer, vengono gestiti dal sistema operativo.
È pertanto opportuno impostarli in modo che:

- lo schermo venga spento automaticamente dopo alcuni minuti di inattività
- il computer venga sospeso (o ibernato) dopo un certo periodo di inattività.

APPROFONDIMENTO

In Windows 7 le opzioni di risparmio energetico si possono regolare mediante l'applet **Opzioni di risparmio energia** del Pannello di controllo.

Per impostazione predefinita, Windows 7 offre tre combinazioni di risparmio energetico: **Bilanciato**, **Risparmio energia** e **Prestazioni elevate**. È inoltre possibile creare una combinazione personalizzata di energia cliccando sul link omonimo nella barra laterale a sinistra. Ogni piano predefinito può comunque essere cambiato selezionando il link **Modifica impostazioni combinazione**. Essenzialmente ogni combinazione prevede un tempo per la disattivazione dello schermo e un tempo per la sospensione del computer. Nelle impostazioni avanzate si può regolare in maniera più fine il risparmio energetico di molti componenti interni del computer quali disco rigido, scheda wireless, porte USB, processore, ecc.

Per quanto riguarda invece i termini utilizzati, di seguito è data una breve spiegazione dei termini Sospensione e Ibernazione.

Sospensione: in questa modalità, il computer non si spegne completamente e usa ancora piena energia per alimentare la RAM e tenere in memoria i dati ed i programmi aperti. Monitor e hard disk sono spenti, ma non appena si tocca il mouse, il computer si sveglia.

Ibernazione: in questa modalità il computer si spegne ma prima salva tutto il contenuto della RAM sul disco rigido. Quando si riavvia il computer, la RAM viene caricata dall'hard disk, in modo che si possa continuare a lavorare dal punto in cui si era rimasti.

Il riciclo di cartucce, carta e dispositivi elettronici

È noto che i rifiuti elettronici contengono sostanze come piombo, cadmio e mercurio, pericolose per l'ecosistema e, quindi, per l'uomo. Se si pensa al numero di dispositivi elettronici che nell'arco di un anno vengono sostituiti sia nelle grandi organizzazioni, sia da privati, si percepisce chiaramente quanto sia importante riutilizzare ciò che è riciclabile.

Non è possibile provvedere autonomamente alla rottamazione del proprio PC, ma è necessario rivolgersi a ditte specializzate sia nel recupero del materiale inquinante che nello smaltimento, nel rispetto della normativa vigente.
Analogamente, per quanto riguarda la carta, non va buttata ma riciclata.

Per ogni eventuale dubbio in proposito, i cittadini e le aziende possono rivolgersi all'A.N.P.A., **Agenzia Nazionale per la Protezione dell'Ambiente**, che ha predisposto in merito alcune linee guida.

APPROFONDIMENTO

Sono molti gli elementi che possono essere riciclati. Consegnando computer e le periferiche non più funzionanti alle apposite ditte o conferendole presso le piattaforme ecologiche queste apparecchiature saranno smontate in modo da separare plastica, metallo, vetro e metalli rari.

Non va altresì dimenticato che anche le cartucce o il toner delle stampanti sono molto inquinanti. I contenitori infatti possono essere ricaricati e riutilizzati. Molte aziende hanno appositi programmi di ritiro e incentivano le sostituzioni con forti sconti sul riciclato.

Da ultimo, benché le nuove batterie abbiano un contenuto ridotto di metalli pesanti, costituiscono sempre un rischio per l'ambiente e devono essere smaltite negli appositi contenitori che saranno poi conferiti al consorzio di smaltimento abilitato.

Come ulteriore aiuto, dal 2010 è possibile riconsegnare **gratuitamente** un rifiuto elettronico prodotto in ambito domestico direttamente al rivenditore all'atto dell'acquisto di un'apparecchiatura della medesima tipologia; tale procedura è definita "**uno contro uno**". Lo prevede un decreto del ministero dell'ambiente per raggiungere gli obiettivi di recupero fissati a livello comunitario.

Migliorare l'accessibilità al computer

Il computer può aiutare molto le persone che hanno disabilità soprattutto sensoriali o motorie. Per questo motivo sono stati scritti dei software che facilitano l'accesso a chi qualche tipo di disabilità.

Ad esempio, in Windows 7 il "**Centro accessibilità**" attivabile dal pannello di controllo fornisce diversi strumenti tra cui **l'assistente vocale**, per la lettura dello schermo, la **lente di ingrandimento**, per ingrandire la porzione dello schermo vicino al puntatore del mouse, o la **tastiera su schermo**, per utilizzare il mouse o altri dispositivo che interagiscano con la tastiera.