

**AGENZIA REGIONALE DELL'ABRUZZO
PER LA COMMITTENZA**



**DISCIPLINARE INTERNO PER L'UTILIZZO
DI INTERNET E DELLA POSTA
ELETTRONICA DA PARTE DEI DIPENDENTI**

AGOSTO 2023

Sommario

ARTICOLO 1 – OGGETTO	3
ARTICOLO 2 - PRINCIPI	3
ARTICOLO 3 - DEFINIZIONI	4
ARTICOLO 4 - MODALITÀ DI ACCESSO E DI UTILIZZO DELLA POSTAZIONE DI LAVORO	4
ARTICOLO 5 - INTERNET	6
ARTICOLO 6 - POSTA ELETTRONICA	7
ARTICOLO 7 - CONTROLLI	9
ARTICOLO 8 - PUBBLICAZIONE DI CONTENUTI E REALIZZAZIONE DI SITI PERSONALI	10
ARTICOLO 9 - INTERRUZIONE E CESSAZIONE D’UFFICIO DEL SERVIZIO	10
Art. 10 - DIFESA DAL RANSOMWARE	11
Art. 11 - UTILIZZO SISTEMI DI VIDEOCONFERENZE	12
Art. 12 - GLOSSARIO	12

ARTICOLO 1 - OGGETTO

Il presente disciplinare, adottato sulla base delle indicazioni contenute:

- ✓ nel provvedimento di data 1 marzo 2007 (in G.U. n. 58 di data 10 marzo 2007) del Garante per la protezione dei dati personali, riguardante il *Trattamento di dati personali relativo all'utilizzo di strumenti elettronici da parte dei lavoratori*;
- ✓ nella Direttiva n. 2 del 26 maggio 2009 del Ministro per la Pubblica Amministrazione e l'Innovazione;

ha per oggetto i criteri e le modalità operative di accesso e di utilizzo del servizio Internet e di posta elettronica da parte dei dipendenti dell'Agenzia Regionale dell'Abruzzo per la Committenza (nel seguito Agenzia) - e di tutti gli altri soggetti che a vario titolo operano nelle strutture e sedi operative dell'Agenzia (lavoratori socialmente utili, collaboratori, tirocinanti, stagisti).

ARTICOLO 2 - PRINCIPI

Il presente disciplinare viene predisposto nel rispetto della vigente disciplina in materia di Privacy, con riguardo, in particolare, alle norme del Regolamento europeo GDPR n. 2016/679.

L'Agenzia garantisce che il trattamento dei dati personali dei dipendenti, effettuato per verificare il corretto utilizzo della Posta elettronica e di Internet, si conforma ai seguenti principi:

1. il principio di *necessità*, secondo cui i sistemi informativi e i programmi informatici devono essere configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi in relazione alle finalità perseguite (par. 5.2 del Provvedimento);
2. il principio di *correttezza*, secondo cui le caratteristiche essenziali dei trattamenti devono essere rese note ai lavoratori (art. 5 GDPR) poiché le tecnologie dell'informazione, in modo più marcato rispetto ad apparecchiature tradizionali, permettono di svolgere trattamenti ulteriori rispetto a quelli connessi ordinariamente all'attività lavorativa, anche all'insaputa o, comunque, senza la piena consapevolezza dei lavoratori (par. 3 del Provvedimento);
3. il principio di *pertinenza e non eccedenza* (par. 6 del Provvedimento), in virtù del quale: i trattamenti devono essere effettuati per finalità determinate, esplicite e legittime (art. 5 GDPR; par. 4 e 5 del Provvedimento);
4. il datore di lavoro deve trattare i dati "nella misura meno invasiva possibile";
5. le attività di monitoraggio devono essere svolte solo da soggetti preposti (par. 8 del Provvedimento) e essere focalizzate sull'area di rischio, tenendo conto della normativa in

materia di protezione dei dati personali e, se pertinente, del principio di segretezza della corrispondenza (Parere n. 8/2001, punti 5 e 12).

ARTICOLO 3 - DEFINIZIONI

Nel presente documento si intende per:

- UTENTE INTERNET: persona autorizzata ad accedere al servizio Internet anche al di là dei siti istituzionali eventualmente preventivamente selezionati (white list) dall'Ente, con l'unico limite di filtri predeterminati che si attivano in modo automatico durante la navigazione;
- UTENTE DI POSTA ELETTRONICA: persona autorizzata ad accedere al servizio di posta elettronica;
- WHITE LIST: elenco di siti direttamente e immediatamente accessibili da tutti gli utenti Internet;
- BLACK LIST: elenco di siti non accessibili da nessun utente;
- INTERNET PROVIDER: azienda che fornisce all'Ente il canale di accesso alla rete Internet;
- POSTAZIONE DI LAVORO: personal computer collegato alla rete dell'Ente tramite il quale l'utente accede ai servizi;
- LOG: archivio delle attività di consultazione in rete.

ARTICOLO 4 - MODALITÀ DI ACCESSO E DI UTILIZZO DELLA POSTAZIONE DI LAVORO

La configurazione dei servizi di accesso a Internet viene eseguita esclusivamente dai tecnici dei Servizi Informatici della sede operativa competente per materia, che può anche essere affidato a Ditta esterna all'Amministrazione. Le postazioni di lavoro sono preventivamente individuate e assegnate personalmente a ciascun dipendente; per accedere ai servizi informatici dell'Ente dalla postazione di lavoro, garantendone quindi la sua protezione, il dipendente dovrà utilizzare le credenziali di accesso del sistema di autenticazione in uso presso la sede di svolgimento del servizio: in riferimento agli uffici dell'Agenzia di Tortoreto, l'accesso è basato su tecnologia RADIUS/TACACS, conformemente alle prescrizioni di sicurezza generali adottate dall'Agenzia. Superato il sistema di autenticazione, il dipendente sarà collegato alla rete dell'Ente e ad Internet per l'accesso alle risorse consentite dalla profilazione.

Per quanto attiene alle altre Sedi Operative di Pescara e L'Aquila, l'accesso alla rete avverrà secondo le linee guida e le policy regionali in uso presso di esse, come stabilito dalle rispettive strutture

competenti per materia (ad esempio autenticazione su dominio degli utenti).

Su richiesta del dirigente di competenza, ai dipendenti potrà essere garantito accesso alle risorse aziendali attraverso tecnologie VPN (IPSEC Remote Access), attraverso autenticazione sulla medesima piattaforma di gestione RADIUS/TACACS, prediligendo criteri di temporizzazione correlati all'effettiva durata di espletamento del servizio.

Il dipendente, preso atto che la conoscenza della password da parte di terzi consente a questi ultimi di accedere alla rete dell'Ente, nonché l'utilizzo dei relativi servizi in nome del titolare e l'accesso ai dati a cui egli stesso è abilitato, si impegna a:

1. non cedere, una volta superata la fase di autenticazione, l'uso della propria stazione a personale non autorizzato, in particolar modo per quanto riguarda l'accesso a Internet e ai servizi di posta elettronica;
2. non lasciare incustodita ed accessibile la propria postazione una volta connesso al sistema con le proprie credenziali di autenticazione;
3. conservare la password nella massima riservatezza e con la massima diligenza;
4. non utilizzare credenziali (user-id e password) di altri utenti, nemmeno se fornite volontariamente o di cui si ha casualmente conoscenza;
5. mantenere la corretta configurazione del proprio computer non alterando le componenti hardware e software predisposte allo scopo né installando ulteriori software non autorizzati;
6. non salvare file audio, video e file non istituzionali di qualsiasi tipo nelle connessioni di rete su cui viene eseguito giornalmente il back-up;
7. non installare o non utilizzare programmi di sistema, applicativi o gestionali privi di regolare contratto di licenza d'uso sottoscritto dall'Ente, salvo specifica autorizzazione in tal senso da parte del Responsabile;
8. non modificare le configurazioni (in modo particolare l'identificativo in rete del proprio Pc impostato dall'Amministratore di sistema);
9. non installare sul proprio Pc dispositivi hardware personali (modem, schede audio etc.), salvo specifica autorizzazione in tal senso da parte del Responsabile;
10. mantenere il programma antivirus sempre attivo con riferimento all'ultima versione disponibile. In caso di impossibilità ad operare in tal senso è necessario fornire immediata segnalazione al proprio Responsabile;
11. non utilizzare strumenti software e/o hardware atti ad intercettare il contenuto delle comunicazioni informatiche all'interno dell'Ente. Per ciò che concerne l'utilizzo di supporti

magnetici e ottici, il dipendente deve attenersi alle seguenti disposizioni:

- non è consentito scaricare files (programmi, archivi di dati, etc.) contenuti in supporti magnetici e/o ottici che non abbiano attinenza con la propria prestazione lavorativa;
- è fatto obbligo di sottoporre a controllo preventivo tutti i file di provenienza incerta o esterna, attinenti l'attività lavorativa.

Per prevenire la manomissione della configurazione hardware e software delle postazioni di lavoro, salvo rari casi necessari per il funzionamento di specifici applicativi, gli utenti sono configurati con diritti limitati, diversi da quelli di amministratore.

Qualsiasi azione svolta utilizzando il codice identificativo e/o la password sarà assegnata in termini di responsabilità all'utente assegnatario del codice. L'utente sarà civilmente responsabile di qualsiasi danno arrecato alla Amministrazione e all'Internet provider e/o a terzi in dipendenza della mancata osservazione di quanto previsto dal presente disciplinare.

L'utente, inoltre, potrà essere chiamato a rispondere civilmente, oltre che per i propri fatti illeciti, anche per quelli commessi da chiunque utilizzi il suo codice identificativo e/o password, con particolare riferimento all'immissione in rete di contenuti critici o idonei a offendere l'ordine pubblico o il buon costume così come definiti dalla giurisprudenza della Corte di Cassazione.

La violazione delle presenti disposizioni può comportare infine l'applicazione delle sanzioni disciplinari previste dal vigente contratto collettivo provinciale di lavoro, rimanendo ferma ogni ulteriore forma di responsabilità penale.

ARTICOLO 5 - INTERNET

Tutti i dipendenti cui è assegnata una postazione di lavoro per assolvimento di funzioni istituzionali, a prescindere dalla sede operativa presso la quale esse sono fisicamente svolte - limitatamente alle risorse consentite dai dispositivi di sicurezza e di frontiera, e previa identificazione con le modalità illustrate nell'art. 4 - possono utilizzare Internet. Il dipendente-utente è direttamente e totalmente responsabile dell'uso che egli fa del servizio di accesso a Internet, dei contenuti che vi ricerca, dei siti che contatta, delle informazioni che vi immette e delle modalità con cui opera.

L'eventuale lista dei siti da raggiungere (WHITE LIST) sarà implementata dinamicamente nel tempo su richiesta dei responsabili dei servizi dell'Ente.

Al fine di prevenire o comunque limitare il rischio di utilizzi impropri della rete, l'Ente dispone anche di tecnologie (i.e. URL filtering) e dispositivi (firewall, IPS, IDS) che impediscono l'accesso diretto

a siti illeciti e/o dannosi che sicuramente non hanno natura istituzionale.

Al dipendente-utente Internet non è consentito:

1. servirsi o dar modo ad altri di servirsi della stazione di accesso a Internet per attività non istituzionali, per attività poste in essere in violazione del diritto d'autore o altri diritti tutelati dalla normativa vigente;
2. effettuare transazioni finanziarie, operazioni di remote banking, acquisti on line e simili, se non attinenti l'attività lavorativa o direttamente autorizzati dal Responsabile;
3. utilizzare sistemi Peer to Peer (P2P), di file sharing, podcasting, webcasting, torrent o similari, così come connettersi a siti che trasmettono programmi in streaming (come radio o TV via WEB) senza essere stati preventivamente autorizzati dal dirigente di competenza;
4. scaricare software gratuiti (freeware, shareware, public domain etc.) dalla rete, salvo casi di comprovata utilità (es: antivirus) ed in ogni caso previa autorizzazione in tal senso da parte del Responsabile che, dopo aver verificato il rispetto delle condizioni di licenza, provvederà a eseguire fisicamente lo scarico in modalità sicura e consegnare il software al richiedente, facendo sì che venga installato da personale competente;
5. utilizzare Internet provider diversi da quello scelto ufficialmente dall'Ente e la connessione di stazioni di lavoro aziendali alle reti di detti provider con sistemi di connessione diversi (es. modem) da quello centralizzato;
6. registrarsi a siti i cui contenuti non siano attinenti con l'attività lavorativa;
7. partecipare a forum e/o l'utilizzo di chat se non per motivi strettamente attinenti l'attività lavorativa;
8. usare la rete in modo difforme da quanto previsto dal presente documento e dalle leggi penali, civili e amministrative in materia di disciplina dell'attività e dei servizi svolti sulla rete.

ARTICOLO 6 - POSTA ELETTRONICA

Il servizio di posta elettronica viene fornito per consentire la comunicazione con soggetti terzi interni ed esterni all'Ente e in stretta connessione con l'effettiva attività e mansione del soggetto autorizzato.

Al fine di non compromettere la sicurezza dell'Ente e di prevenire conseguenze legali a carico dello stesso è necessario che i soggetti autorizzati adottino le seguenti norme comportamentali per le caselle di posta elettronica personale e nominativa fornite dall'Ente e per le caselle di servizio il cui accesso è garantito al solo personale previamente designato e autorizzato dal Dirigente di competenza.

In caso di assenza dal lavoro del dipendente-utente per brevi periodi, è a disposizione una apposita

funzionalità di sistema che consente di inviare automaticamente un messaggio di risposta che avvisa il mittente dell'assenza del destinatario, individuando eventualmente altre modalità di contatto con la struttura.

Per le sole caselle di servizio, in caso di assenza del personale delegato o dove non sia stata attivata la procedura di cui sopra, su eventuale richiesta del Dirigente di competenza, la relativa delega può essere estesa ad un altro dipendente dell'ufficio al fine di verificare il contenuto dei messaggi e ad inoltrare al Responsabile del servizio quelli ritenuti rilevanti e per lo svolgimento dell'attività lavorativa.

Al dipendente:

1. non è consentito utilizzare la posta elettronica per motivi non attinenti allo svolgimento delle mansioni assegnate;
2. non è consentito l'utilizzo dell'indirizzo di posta elettronica istituzionale per la partecipazione a dibattiti, forum, mail-list, salvo specifica autorizzazione in tal senso da parte del Responsabile dei Servizi Informatici;
3. è vietato utilizzare tecniche di "mail spamming" cioè di invio massiccio di comunicazioni a liste di distribuzione extra aziendali o di azioni equivalenti;
4. è vietato utilizzare il servizio di posta elettronica per inoltrare giochi, scherzi, barzellette, appelli e petizioni (anche se possono sembrare veritieri e socialmente utili), catene di S. Antonio ed altri messaggi che non siano attinenti al lavoro;
5. è vietato allegare al testo delle comunicazioni materiale potenzialmente insicuro (ad es. programmi, scripts, macro), così come file di dimensioni eccessive;
6. è vietata l'apertura di allegati di non comprovata origine. Il ricevimento di detti messaggi deve essere tempestivamente segnalato al Responsabile dei Servizi Informatici;
7. è vietata l'apertura di link contenuti all'interno di messaggi a meno di comprovata sicurezza sul contenuto dei siti richiamati.

In ogni caso nell'ipotesi in cui l'email ricevuta preveda mittenti non conosciuti, allegati di dubbia natura e informazioni riservate sia nell'oggetto che nel corpo dei messaggi occorre procedere con una valutazione approfondita circa gli elementi di sicurezza minime per l'utilizzo del servizio di posta elettronica ed in particolare l'accertamento di attività non consentite e/o illecite.

Di conseguenza, ad esempio, nel ricevere un file allegato ai messaggi è sempre necessario assicurarsi che l'antivirus sia attivo e che qualora i sistemi di sicurezza evidenzino anche potenziali anomalie e/o non si abbia contezza del mittente né del materiale inviato lo stesso potrà essere utilizzato unicamente

in un ambiente protetto o previa verifica diretta con il mittente.

L'utilizzo di liste di distribuzione riservate, comunemente riunite nella - Rubrica "gruppi", che permettono l'invio di e-mail a una pluralità di utenti o a tutti gli utenti, è consentito solo a determinati soggetti, su autorizzazione del Dirigente / Responsabile dell'Ufficio.

ARTICOLO 7 - CONTROLLI

L'Ente, utilizzando sistemi informativi per esigenze produttive o organizzative (ad es. per rilevare anomalie o per manutenzioni) o, comunque, quando gli stessi si rivelano necessari per la sicurezza sul lavoro, può avvalersi legittimamente nel rispetto dell'art. 4, comma 2 dello Statuto dei Lavoratori, di sistemi che consentano indirettamente un controllo a distanza (cd. controllo preterintenzionale), e determinano un trattamento di dati personali riferiti o riferibili ai lavoratori, nel rispetto di quanto previsto dal paragrafo 5 del Provvedimento del Garante. In ogni caso l'Ente adotta una specifica policy per evitare che ogni attività di controllo per ragioni di sicurezza sia conforme alle normative sulla protezione dei dati personali e alle limitazioni imposte sul controllo delle attività lavorative.

Le comunicazioni effettuate attraverso il servizio di posta elettronica interno sono riservate.

L'Ente non effettua in alcun caso trattamenti di dati personali mediante sistemi hardware e software che mirano al controllo a distanza dei lavoratori grazie ai quali sia possibile ricostruire la loro attività e che vengano svolte tramite i seguenti mezzi:

- lettura e registrazione sistematica dei messaggi di posta elettronica dei dipendenti ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per fornire e gestire il servizio di posta elettronica;
- riproduzione e eventuale memorizzazione sistematica delle pagine web visualizzate dal dipendente;
- lettura e registrazione dei caratteri inseriti dai lavoratori tramite la tastiera ovvero dispositivi analoghi a quello descritto;
- analisi occulta dei dispositivi per l'accesso a Internet o l'uso della posta elettronica messi a disposizione dei dipendenti.

Le attività sull'uso del servizio di accesso ad Internet vengono automaticamente registrate in forma elettronica attraverso i LOG di sistema, che possono riguardare:

- registro eventi del sistema operativo client;
- messaggi di registro middleware (Active Directory, proxy, dominio, RADIUS, etc.);
- log dei sistemi di frontiera (Firewall, etc.).

Il trattamento dei dati contenuti nei LOG può avvenire esclusivamente in forma anonima in modo tale da precludere l'identificazione degli utenti e/o delle loro attività.

I dati anonimi aggregati, riferibili all'intera struttura o a sue aree, sono a disposizione del Titolare del trattamento o suo delegato per le valutazioni di competenza.

I dati personali contenuti nei log possono essere trattati in via eccezionale e tassativamente nelle seguenti ipotesi:

- per corrispondere ad eventuali richieste della polizia postale e/o dell'autorità giudiziaria;
- su richiesta del Titolare del trattamento o suo delegato quando si verifichi un evento dannoso o una situazione di pericolo che richieda un immediato intervento;
- su richiesta del Titolare del Trattamento o suo delegato per specifici casi di utilizzo anomalo degli strumenti forniti dall'Ente ed in conformità con le normative nazionali ed europee sulla protezione dei dati personali e sugli strumenti di sicurezza dei sistemi informativi.

I dati contenuti nei LOG sono conservati per il tempo necessario al perseguimento di finalità organizzative, produttive e di sicurezza, comunque non inferiore a sei mesi.

I dati riguardanti il software installato sulle postazioni di lavoro, senza alcuna indicazione dell'utente che ha effettuato l'installazione, possono essere trattati per finalità di verifica della sicurezza dei sistemi e di controllo del rispetto delle licenze regolarmente acquistate.

ARTICOLO 8 - PUBBLICAZIONE DI CONTENUTI E REALIZZAZIONE DI SITI PERSONALI

Il dipendente-utente non è autorizzato a produrre e pubblicare propri siti web. Ogni eventuale necessità di realizzare siti web personali o di struttura dovrà essere espressamente autorizzata dal Titolare del trattamento o suo delegato.

Il dipendente-utente si obbliga a tenere indenne l'Amministrazione da tutte le perdite, danni responsabilità, costi, oneri e spese, ivi comprese le eventuali spese legali, che dovessero essere subite o sostenute quali conseguenze di qualsiasi inadempimento da parte dell'utente agli obblighi e garanzie previste nel precedente paragrafo e comunque connesse alla immissione delle informazioni in Internet anche in ipotesi di risarcimento danni pretesi da terzi a qualunque titolo.

ARTICOLO 9 - INTERRUZIONE E CESSAZIONE D'UFFICIO DEL SERVIZIO

Il servizio di Internet e posta elettronica può essere interrotto per le manutenzioni ordinarie e straordinarie; le interruzioni saranno preventivamente comunicate agli utenti, salvo casi di forza

maggiore.

Ai sensi della presente disciplina, l'utilizzo del servizio di accesso ad Internet cessa d'ufficio nei seguenti casi:

- se non sussiste più la condizione di dipendente o collaboratore autorizzato o non è confermata l'autorizzazione all'uso;
- se è accertato un uso non corretto del servizio da parte del dipendente-utente o comunque un uso estraneo ai suoi compiti professionali;
- se vengono sospettate manomissioni e/o interventi sul hardware e/o sul software del dipendente-utente impiegati per la connessione compiuti eventualmente da personale non autorizzato;
- in caso di diffusione o comunicazione imputabili direttamente o indirettamente al dipendente-utente, di password, procedure di connessione, indirizzo IP ed altre informazioni tecniche riservate;
- in caso di accesso doloso del dipendente-utente a directory, a siti e/o file e/o servizi da chiunque resi disponibili non rientranti fra quelli per lui autorizzati e in ogni caso qualora l'attività del dipendente-utente comporti danno, anche solo potenziale al sito contattato;
- in caso di concessione di accesso ad Internet diretta o indiretta a qualsiasi titolo da parte del dipendente-utente a terzi;
- in caso di violazione e/o inadempimento imputabile al dipendente-utente di quanto stabilito nei precedenti punti;
- in ogni altro caso in cui sussistono ragionevoli evidenze di una violazione degli obblighi del dipendente-utente.

Art. 10 - DIFESA DAL RANSOMWARE

Il ransomware è un programma informatico dannoso ("malevolo") che può "infettare" un dispositivo digitale (PC, tablet, smartphone, smart TV), bloccando l'accesso a tutti o ad alcuni dei suoi contenuti (foto, video, file, ecc.) per poi chiedere un riscatto (in inglese, "ransom") da pagare per "liberarli".

È vietato aprire messaggi provenienti da soggetti sconosciuti o con i quali non si hanno rapporti e, in ogni caso, se si hanno dubbi, non si deve cliccare su link o banner sospetti e non si devono aprire allegati di cui si ignora il contenuto.

Art. 11 - UTILIZZO SISTEMI DI VIDEOCONFERENZE

I sistemi di videoconferenza sono strumenti di lavoro da utilizzare in alternativa a riunioni in presenza o come alternativa alla chiamata telefonica. In ogni caso anche i sistemi di videoconferenza valgono le norme di riservatezza e protezione dei dati personali oltre alle generali norme di sicurezza informatica. Ad esempio è vietato riprendere documenti contenenti dati personali o dati riservati senza specifica autorizzazione e di condividere tali dati mediante la visione dei documenti in ambiente videoconf. In tutti i casi è comunque necessario assicurarsi che i soggetti partecipanti siano quelli autorizzati e qualora sia necessario procedere e/o utilizzare registrazioni audio video che tali attività siano consentite dalle normative e/o abbiano utilizzato preventivamente una base giuridica personalizzata per gli specifici eventi.

Art. 12 - GLOSSARIO

Backup: il termine, che significa copia di sicurezza, indica l'operazione di duplicare su differenti supporti di memoria le informazioni (dati o programmi) presenti sui dischi di una stazione di lavoro o di un server. Normalmente viene svolta con una periodicità stabilita.

Chat: (letteralmente, "chiacchierata") è un servizio informatico che permette attraverso Internet, di attivare e gestire un dialogo in tempo reale fra due o più utenti utilizzando principalmente messaggi testuali.

File sharing: condivisione di file all'interno di una rete comune.

Forum: generalmente si riferisce ad un archivio informatico contenente discussioni e messaggi scritti dagli utenti oppure al software utilizzato per fornire questo archivio. Ci si riferisce comunemente ai forum anche come board, message board, bulletin board, gruppi di discussione, bacheche e simili.

Guestbook: (letteralmente, libro degli ospiti) è un servizio interattivo che permette ai visitatori di un sito web di poter lasciare 'firme' e commenti.

ID utente: codice identificativo personale per l'accesso ai sistemi informatici. Normalmente è formato dal cognome o dal cognome e parte del nome.

LOG: il termine, che significa giornale di bordo o semplicemente giornale, viene utilizzato nell'informatica per indicare la registrazione cronologica delle operazioni man mano che vengono eseguite ed il file su cui tali registrazioni sono memorizzate.

Mailing-list: (letteralmente, lista per corrispondenza traducibile in italiano con lista di diffusione) è un sistema organizzato per la partecipazione di più persone in una discussione tramite posta elettronica.



Mail spamming: è l'invio di grandi quantità di messaggi indesiderati (generalmente commerciali). Può essere messo in atto attraverso qualunque media, ma il più usato è Internet attraverso l'e-mail.

Password: (in italiano: “parola chiave”, “parola d'ordine”, o anche “parola d'accesso”) è una sequenza di caratteri utilizzata per accedere ad una risorsa informatica.

Podcasting: sistema che permette di scaricare in modo automatico documenti (generalmente audio o video) chiamati podcast, utilizzando un programma generalmente gratuito chiamato aggregatore o feeder. Con podcast si intende un file (generalmente audio o video), messo a disposizione su Internet e scaricabile automaticamente.

Ransomware: programma informatico che può “infettare” un dispositivo digitale bloccando l'accesso a tutti o ad alcuni dei suoi contenuti per poi chiedere un riscatto (in inglese, “ransom”) da pagare per “liberarli”.

Software freeware: programmi software distribuiti in modo gratuito.

Software peer-to-peer: programmi utilizzati per la condivisione e lo scambio di files fra elaboratori. Questi programmi vengono utilizzati principalmente per scambiarsi file di tipo mp3, (file musicali) e DivX o mkv (contenenti i film) spesso in violazione dei diritti d'autore.

Stand-alone: si riferisce ad un'apparecchiatura capace di funzionare da sola, indipendentemente dalla presenza di altre apparecchiature con cui potrebbe comunque interagire.

Streaming: identifica un flusso di dati audio/video trasmessi da una sorgente a una o più destinazioni tramite una rete telematica. Questi dati vengono riprodotti man mano che arrivano a destinazione.

Videoconferenza: Si definisce videoconferenza la combinazione di due tecnologie, dove si ha l'interazione sincrona in audio, video e dati fra due o più soggetti.

Webcast/Webcasting: descrive la trasmissione di segnale audio o video, in tempo reale o ritardato, mediante tecnologie web. Il suono o il video sono catturati con sistemi audio-video convenzionali, quindi digitalizzati e inviati in streaming su un web server. Un client webcast consente agli utenti di connettersi ad un server che sta distribuendo (operazione detta di webcasting) e di ascoltare o visualizzare il contenuto audio/video.

Luogo e data

Il dipendente (per accettazione)
