2020

VADEMECUM PER LA DIDATTICA ONLINE

BUONE PRATICHE, ELEMENTI DI SICUREZZA, ETIQUETTE

PER INSEGNANTI E STUDENTI

[V. 1.1]

morolabs

Sommario

Premessa

L'emergenza creata dalla diffusione del virus COVID-19 ha colto tutti di sorpresa. La dovuta sospensione dell'attività didattica ha stimolato da un lato il cosiddetto lavoro "agile" e dall'altro, sfruttando le tecnologie disponibili, la didattica a distanza e, in alcuni casi, anche l'e-learning.

In questa particolare situazione, il paese paga i mancati investimenti in infrastrutture, in termini di datacenter e piattaforme pubbliche nonché in termini di connettività Internet specie nel cosiddetto "ultimo miglio", prerequisito essenziale tanto per la fruizione dei materiali in modalità asincrona che per la partecipazione alle lezioni sincrone via *conference call* con una qualità audio/video accettabile.

L'introduzione delle nuove piattaforme nella didattica, apparentemente semplici e funzionali, pronte dopo pochi "click", dal facile accesso e per la più ampia condivisione dei materiali ma con *disclaimer* (dichiarazione di esclusione di responsabilità) sempre in un inglese, dal piglio giuridico e ai più del tutto incomprensibili, presenta dei rischi legati al "*digital divide"* culturale tanto quanto ai dispositivi e alle tecnologie utilizzate.

Il presente vademecum, pur nella convinzione di non poter essere totalmente esaustivo sul tema, sia per l'aumento vertiginoso in numero dei sistemi sia per la continua evoluzione delle funzionalità disponibili, vuol tentare di essere da stimolo a comportamenti proattivi di tutti gli attori in modo da ridurre progressivamente la superficie di esposizione ai rischi nell'utilizzo delle piattaforme.

Sono, inoltre, fornite indicazioni ulteriori e buone pratiche per la migliore fruizione possibile dei contenuti, per garantire la continuità dei servizi, per massimizzare le prestazioni e di conseguenza l'efficacia degli strumenti nei processi di apprendimento.

Le famiglie, il corpo docente e i ragazzi sono invitati a segnalare eventuali elementi non compresi nella presente guida, che potranno essere progressivamente integrati fino a raggiungere un livello di completezza e quindi di copertura delle situazioni prevedibili e risolvibili a livello organizzativo e/o comportamentale.

Buon e-Learning, formazione *blended* o formazione a distanza a tutti.

Il Team DPO di Morolabs

Risorse utilizzabili

Nel web sono disponibili moltissime piattaforme utilizzabili in ambito didattico, a volte completamente "gratuite", più spesso gratuite nelle funzionalità base ed estendibili a pagamento oppure versioni *enterprise* o professionali soltanto a pagamento.

È necessario ribadire, riguardo alla gratuità delle piattaforme, che non si tratta né di una operazione filantropica, né di un *give back* mondiale di qualche miliardario americano: è una operazione di marketing, di fidelizzazione, di pagamento di un servizio, talvolta anche ben fatto, con la moneta ufficiale della società delle informazioni ovvero con la cessione dei propri dati e l'accettazione ad essere profilati.

I servizi a pagamento, invece, hanno delle condizioni di utilizzo diverse che non prevedono, a meno di casi particolari, nessuno degli effetti "collaterali" sopra citati.

Nella pratica, le piattaforme maggiormente utilizzate sono le seguenti:

- Google Suite (Gmail, Drive, Calendar, Hangouts Meet, Classroom, etc.)
- WeSchool
- Zoom
- WhatsApp (per le comunicazioni di servizio, lo scambio file e in alcuni casi anche conference)
- Office 365 (in particolare OneDrive per la condivisione dei dati, Skype [in dismissione] sostituito da Teams per le conference)

oltre ai servizi disponibili all'interno della piattaforma del registro elettronico.

I singoli insegnanti possono, esclusivamente in casi di emergenza e al solo fine di garantire un livello di servizio, comunque adeguato, legato alla fase emergenziale, utilizzare anche altre tipologie di piattaforme, servizi di videoconferenza o link a contenuti pubblici.

Ciò deve essere fatto nella consapevolezza dei rischi connessi con un uso indiscriminato delle piattaforme più disparate, alcune delle quali con logiche di business non perfettamente allineate ai principi base della protezione dei dati personali vigenti nella Unione Europea, e giocoforza accettare tali rischi, cercando di non vanificare l'impegno e lo sforzo di tutti rispetto agli obiettivi e, più in generale, alla missione delle istituzioni scolastiche.

Al ritorno ad una condizione di normalità, confidiamo a breve, sarà necessario provvedere ad una razionalizzazione delle piattaforme utilizzate prediligendo le versioni a pagamento, con posizionamento nello spazio UE, sottoposto quindi alla normativa GDPR o, in alternativa, che adottino almeno le Clausole Standard previste per l'esportazione dei dati al di fuori dell'Unione europea.

Principi

I principi che hanno ispirato il presente vademecum sono i seguenti:

1. Tutela dei diritti, delle libertà e della dignità delle persone;
2. Garanzia della necessaria *continuità operativa* per il miglior funzionamento degli strumenti utilizzati;
3. Minor dispendio possibile di energie (umane, tecnologiche, temporali ed economiche);
4. Tutela del patrimonio informativo dell'organizzazione, anche se in formato non strutturato, riduzione dei rischi connessi al trattamento dei dati personali e quindi della probabilità di:
    a. Accessi illegittimi ai sistemi o agli applicativi;
    b. Modifiche indesiderate alle informazioni;
    c. Perdita della disponibilità dei dati;
5. Conformità normativa e allineamento agli standard di mercato;

6. Riduzione della superficie di esposizione rispetto alle vulnerabilità ovvero a quelle debolezze sistemiche trasformabili in un evento indesiderato nel caso si attui una minaccia;
7. Corretto bilanciamento tra usabilità e sicurezza, adottando contromisure basate sull'Analisi dei rischi;
8. Adozione della Regola del minimo previlegio rispetto alla finalità in ottica di stratificazione della Sicurezza;
9. Diritto alla disconnessione degli utilizzatori dai sistemi *mobile*, al di fuori dell'orario di studio o di lavoro.

Condotta e utilizzo etico delle piattaforme da parte degli STUDENTI

Le piattaforme sono fornite agli utilizzatori al fine di sostituire momentaneamente la didattica frontale e, finita l'emergenza, come strumento di condivisione della conoscenza.

Gli utilizzatori sono responsabili dell'utilizzo delle piattaforme in modo eticamente corretto, sicuro, conforme alle disposizioni di legge nonché conforme alle indicazioni del presente vademecum, tenendo nella massima considerazione i diritti, le libertà fondamentali, la sensibilità delle persone come anche gli obiettivi formativi che la scuola deve perseguire.

L'utilizzatore delle piattaforme è direttamente responsabile di tutte le attività effettuate con le credenziali di accesso ricevute, con particolare riguardo alle informazioni inviate o richieste, caricate o visualizzate negli spazi condivisi.

All'utilizzatore delle piattaforme **sono tassativamente vietate tutte le attività non conformi alla legge e, in particolar modo, le seguenti attività**:

1) la creazione, il caricamento o la trasmissione di qualsiasi materiale o documento, in qualsiasi formato (testo, immagine, audio, video), che possa essere ragionevolmente ritenuto offensivo, diffamatorio o osceno;
2) la creazione, il caricamento o la trasmissione di materiali o documenti in qualsiasi formato (testo, immagine, audio, video), che possano ragionevolmente essere ritenuti suscettibili di molestare, intimidire, danneggiare o turbare qualcuno;
3) l'invio di dati di tipo sensibile su canali non sicuri (un esempio di strumento da evitare per inviare dati sensibili è la posta elettronica ordinaria, ad esempio Gmail);
4) la creazione o la trasmissione di qualsiasi documento non riconducibile alle funzioni o ai compiti di competenza oppure estraneo alle attività dell'Istituto;
5) l'accesso non autorizzato alle piattaforme, con account non propri o assegnati ad altri soggetti;
6) la condivisione degli inviti alle sessioni formative con soggetti estranei alla classe di appartenenza; eventuali accessi esterni, non specificatamente autorizzati dalla Dirigente Scolastica, saranno segnalati alle autorità competenti per i provvedimenti necessari (si rimanda ai paragrafi "Continuità operativa" e "Il ruolo della Polizia Postale" per ulteriori indicazioni a riguardo);
7) la registrazione del docente o dei compagni (immagini, audio o video) per finalità estranee allo studio come ad esempio la condivisione o la pubblicazione nei social network.

L'introduzione del lavoro agile pone il problema dell'equilibrio tra vita privata e vita professionale, vista la progressiva trasformazione degli strumenti di comunicazione da asincroni a tempo reale. Deve essere riconosciuto all'utilizzatore delle piattaforme il diritto alla disconnessione[1] come anche dai dispositivi *mobile* al di fuori dell'orario di scuola/lavoro.

[1] L'articolo L. 2242-8 del Codice del lavoro francese ("*Code du travail*") modificato dalla legge Loi n° 2016-1088 (*relative au travail, à la modernisation du dialogue social et à la sécurisation des parcours professionnels)* dispone "Le

Anche nell'utilizzo dei sistemi di *instant messaging* (es. WhatsApp) per la gestione delle comunicazioni di servizio, deve essere garantito il diritto alla disconnessione e ciò è demandato alla sensibilità dei singoli nel rispetto della distinzione tra il tempo dedicato alle attività professionali e momenti da riservare alla vita privata e familiare.

Accortezze nella gestione degli inviti alle sessioni formative on-line

È necessario richiamare l'attenzione dei docenti sulle modalità di invito alle sessioni formative on-line in modo che sia garantita la presenza dei soli soggetti autorizzati/invitati, escludendo eventuali disturbatori o *stalker*. In particolare, le uniche modalità di gestione degli inviti permesse sono le seguenti:

- attraverso la piattaforma utilizzata;
- attraverso il registro elettronico.

Altre modalità di invito NON sono permesse, con particolare riguardo ai sistemi di instant messaging (es. gruppi di WhatsApp) come anche le pubblicazioni su pagine social o sul sito web istituzionale; è fondamentale che l'accesso all'invito risulti ad accesso ristretto e tramite autenticazione degli allievi.

Nel caso risultino presenti in una sessione formativa on-line dei soggetti estranei alla classe o peggio all'Istituto, il docente informa i presenti della immediata chiusura della lezione e procede con una nuova schedulazione attraverso modalità sicure sopra indicate. Eventuali soggetti esterni, come ad esempio gli esperti, devono essere specificatamente autorizzati.

Al ripetersi di episodi di *cyber stalking*, *cyber hate/harassment* o di anche semplice *trolling* dovrà essere informata la Dirigente Scolastica per le necessarie valutazioni, eventuali sanzioni disciplinari e la denuncia alla Polizia Postale.

Contenuti gestiti dai DOCENTI

Al fine di tutelare la dignità e le libertà degli allievi, è necessario evitare di salvare negli spazi di condivisione web o file hosting (es. Google Drive) dati personali soprattutto se di natura particolare (sensibile).

Ad esempio, gli insegnanti **NON DEVONO SALVARE** nelle condivisioni web documentazione relativa a:

1. Bisogni Educativi Speciali (disabilità, disturbi evolutivi specifici, svantaggio socioeconomico, linguistico, culturale) e relativi piani didattici, individualizzati o personalizzati;
2. Disturbi Specifici dell'Apprendimento (DSA);
3. Riferimenti a situazioni di "scuola in ospedale" o "istruzione domiciliare" soprattutto se per motivi di salute;
4. Report, relazioni, certificazioni o qualsiasi altro documento relativamente a quanto appena elencato.

Altra accortezza da osservare riguarda, invece, la tipologia di lavori assegnati ai ragazzi, in cui si dovrà evitare la trattazione di temi che riguardano lo stato di salute proprio o dei propri familiari, argomenti dai quali si possano evincere informazioni relative all'origine razziale o etnica, alle opinioni politiche, alle convinzioni religiose o filosofiche, ai dati di carattere giudiziario.

modalità di esercizio da parte del dipendente del proprio diritto alla disconnessione nonché la messa a disposizione di dispositivi che regolano l'utilizzo degli strumenti informatici, al fine di assicurare il rispetto dei tempi di riposo, del periodo di ferie e della vita personale e familiare". In Italia esiste al momento solo un disegno di legge n. 2233 su lavoro autonomo.

Senza voler entrare nel merito della questione di potenziale eccedenza e non pertinenza rispetto alle finalità, è necessario evidenziare come l'utilizzo degli spazi di condivisione web per il salvataggio dei contenuti appena elencati, riguardanti dati personali di natura particolare, debba avvenire invece in modalità sicura semplicemente adottando ad esempio le tecniche di criptazione.

Molti applicativi di uso comune come Word o Excel integrano già funzionalità di protezione/criptazione tramite chiave. La stessa chiave dovrà essere condivisa esclusivamente fra gli utenti autorizzati tramite comunicazione su altro media (es. a voce, via SMS ma non via Gmail se si utilizza Google Drive).

In caso di immagini, audio, video o altre tipologie di file non gestite nativamente in modalità sicura, è possibile acquisire gratuitamente dei prodotti per il salvataggio compresso e criptato (es. WinRAR). In Allegato 1 – Applicativi e Tecniche di criptazione sono disponibili le indicazioni necessarie per la gestione in piena sicurezza dei contenuti dei file.

Identificazione, autenticazione e autorizzazione

Le piattaforme generalmente utilizzano la famiglia di protocolli "AAA" basata sulle funzioni di Autenticazione, Autorizzazione, Accounting.

Conseguentemente l'accesso alle piattaforme è possibile soltanto se l'utilizzatore:

1. è stato prima di tutto ***identificato*** ovvero sono conosciute le sue generalità ed è stato dotato di credenziali utente (nome utente, password e/o PIN);
2. effettua **l'*autenticazione*** tramite immissione delle credenziali, in modo che il sistema possa verificare se l'individuo è chi sostiene di essere;
3. è stato ***autorizzato*** ovvero è stato conferito il diritto ad accedere a specifiche risorse in base al ruolo ricoperto, al profilo e alle specifiche mansioni assegnate.

La responsabilità delle azioni effettuate utilizzando la coppia "nome utente e password e/o PIN" sarà attribuita in termini di responsabilità al soggetto titolare dell'account, a meno di comprovato illecito da parte di terzi. Da ricordare che il Codice penale punisce con pene molto severe, che prevedono la reclusione, coloro che tentano di entrare in un sistema senza autorizzazione o con account non propri.

Gli account di accesso degli allievi, a meno di specifiche limitazioni della piattaforma in uso, devono essere di tipo pseudonimizzati, in modo che non sia possibile ricostruire direttamente l'identità dei soggetti.

Gli account del personale docente devono essere di tipo nominativo per il dovuto riconoscimento, non riutilizzabili da altri soggetti, anche dopo la conclusione del rapporto di lavoro, nel caso di piattaforme gestite direttamente dall'Istituto.

Gli account di accesso hanno, per impostazione predefinita, una scadenza corrispondente alla data di fine dell'anno scolastico. Sarà cura del gestore della piattaforma estenderne la durata, come anche gestire gli account utente per tutto il ciclo di vita (creazione, aggiornamento, nuovi profili di autorizzazione, reset della password, disattivazione una volta concluso il percorso).

La normativa vigente in tema di protezione dei dati, le norme volontarie e le *best practice* di settore impongono di stratificare le possibilità di accesso ai sistemi e ai servizi IT al fine di garantire un adeguato livello di sicurezza. Ad ogni account utente è collegato uno specifico *profilo di autorizzazione* che permette al singolo utilizzatore l'accesso in funzione del proprio ruolo, delle attività a cui è delegato e specificatamente autorizzato da un superiore. Le eventuali estensioni o eccezioni devono essere autorizzate e tracciate.

Il sistema di Autenticazione, Autorizzazione e Registrazione degli accessi ha l'obiettivo di garantire un adeguato livello di sicurezza, conforme a quanto previsto dalla normativa vigente, poiché traccia, separa gli accessi nei livelli previsti, tutelando la riservatezza e l'integrità delle informazioni trattate.

Registrazione delle attività (*accounting*)

A partire dall'accesso alle piattaforme, le attività degli utilizzatori sono registrate in appositi file detti di *log*. Nei sistemi sono memorizzate tutte le singole attività svolte, in particolare le registrazioni riportano l'utente, l'indirizzo della macchina utilizzata da cui è possibile risalire al possessore, l'ora, la data e il dettaglio delle azioni svolte, incluse le operazioni di forzatura degli accessi.

Al fine di contenere lo spazio necessario alla conservazione, i file di log sono conservati in logica di rotazione, ovvero sono sovrascritti al raggiungimento di una certa data o di una certa dimensione; ogni piattaforma potrebbe avere tempistiche di conservazione differente, generalmente attestate sui 12 mesi.

Corretto uso delle Credenziali di autenticazione

Le credenziali di autenticazione sono composte da un codice (account utente) facilmente riconducibile al soggetto e da una *password e/o PIN conosciuti al solo utilizzatore*. ***È tassativamente vietato rivelare la propria password*** di accesso alla piattaforma o ai servizi disponibili.

Da notare che qualsiasi azione effettuata utilizzando la coppia "account utente e password e/o PIN" sarà attribuita in termini di responsabilità all'utente titolare registrato, a meno di comprovato illecito da parte di terzi.

La *lunghezza minima di una password* deve essere di almeno 8 caratteri; considerato che i sistemi di violazione impiegano tempistiche esponenzialmente proporzionali alla lunghezza della password da violare, è necessario considerare almeno 14 caratteri[2] per gli account dei servizi on-line (es. posta elettronica, piattaforme web), in special mondo per le attività di amministrazione di sistema.

Le password non devono essere trascritte; per questo è importante che siano facili da ricordare. È consigliabile utilizzare tecniche di memorizzazione (es. Mi_P1@c3_l4_P1zz@).

È fondamentale utilizzare password diverse per scopi, piattaforme o applicativi diversi. L'eventuale violazione di un sistema potrebbe comportare effetti indesiderati anche su tutti gli altri sistemi utilizzati, di istituto o personali.

Le password devono essere modificate ad intervalli regolari per ridurre l'eventuale finestra temporale di esposizione e comunque almeno ogni 3 mesi (cd. *password aging*).

Le password non devono mai far riferimento a termini di senso compiuto poiché già contenute nei dizionari utilizzati dai sistemi di violazione o essere troppo ovvie (es. 'P@ssword').

Le password non devono essere in alcun modo collegate alla vita privata o lavorativa dell'utilizzatore. Sono quindi da escludere i nominativi dei familiari, la data di nascita, il codice identificativo, la targa dell'auto, la squadra del cuore, il soprannome, ecc. (l'elenco riportato non è esaustivo).

Le password devono contenere combinazioni di caratteri Maiuscoli, minuscoli, numeri e caratteri speciali anche quando non specificatamente richiesto dal sistema utilizzato (complessità).

[2] Misura minima prevista da AgID - «Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)». (17A03060) (GU Serie Generale n.103 del 05-05-2017)

Le password non devono essere riutilizzate a breve distanza di tempo; la rotazione minima prevista è almeno pari a 5 password diverse consecutive (cd. *password history*);

Le password degli account di accesso alle piattaforme non sottoposte alle politiche di complessità, di invecchiamento o di rotazione, devono comunque rispettare le medesime regole, agendo manualmente e confidando nella serietà di tutti.

Le password non devono essere comunicate a nessuno, per nessun motivo, con nessun mezzo (ad esclusione del primo accesso). In caso di problemi di accesso alle risorse fare riferimento al supporto tecnico.

La digitazione delle password deve avvenire in massima sicurezza evitando di mostrare a terzi la sequenza dei tasti premuti. Questa indicazione è fondamentale per tutto il corpo docente.

I colleghi impegnati in attività condivise al computer **sono tenuti a voltarsi** nel caso sia richiesta l'autenticazione al sistema o alla piattaforma software utilizzati.

È vietata la memorizzazione delle password nei browser o tramite applicativi di gestione password, come ad esempio Pocket Password; nel caso si utilizzi Mozilla Firefox è possibile memorizzare le password nel browser solo nel caso di attivazione della funzione 'Utilizza una password principale' inserendo una password estremamente complessa e lunga. Sono comunque esclusi sistemi o applicativi software di memorizzazione delle credenziali nel cloud a meno di garanzia di criptazione ad alto livello.

Non utilizzare strumenti web per la generazione o il controllo del livello di sicurezza (utilizzare eventualmente password con costruzione simile per verificarne la robustezza; es. https://password.kaspersky.com/it).

Per l'invio delle password di criptazione dei file e della documentazione non deve essere mai utilizzato lo stesso media (es. il file criptato viene inviato via posta elettronica e la password comunicata a voce, via telefono).

Non seguire le mode del momento, utilizzare acronimi, pattern ('CristianoRonaldo$' oppure ricorrenza del primo carattere di ogni parola maiuscolo e un dollaro finale), ripetizioni e sequenze ('11111Paperin0000' oppure 'QWERTY12345') o parole presenti nei dizionari facilmente reperibili in Internet.

Le password degli esempi sopra riportate NON sono utilizzabili.

Nel caso di perdita (o anche solo il sospetto di perdita) della segretezza della password è necessario:

1) Modificare immediatamente la password in uso (sui sistemi Windows CTRL+ALT+CANC e Cambia password; verificare le modalità per i singoli applicativi);
2) Nei casi potenzialmente più gravi o dove sono a rischio i dati dell'Istituto, è necessario comunicare l'accaduto al gestore della piattaforma e al DPO per la valutazione della situazione e l'attivazione delle procedure di emergenza per incidente alla sicurezza e data breach al fine di attivare tutti i controlli e le contromisure del caso.

Nel caso l'utilizzatore sbagli per più di 5 volte l'inserimento della password, l'account è automaticamente disabilitato; per effettuare la riabilitazione dell'account è necessario contattare il supporto tecnico.

In caso di prolungato inutilizzo dell'account (per più di 6 mesi), in caso di cessazione o trasferimento degli utilizzatori, il sistema di gestione delle identità provvede all'automatica disabilitazione. L'eventuale riabilitazione dovrà essere autorizzata dal gestore della piattaforma.

Nei casi di particolare emergenza oppure in presenza di comportamenti di alcuni utilizzatori che possano comportare problemi di sicurezza, il gestore della piattaforma è autorizzato alla momentanea disattivazione degli account in questione. Risolta la problematica evidenziata sarà cura del gestore della piattaforma ripristinare le precedenti autorizzazioni concesse.

Le piattaforme hanno integrata la funzione di reset password self-service (che permette la re-impostazione della password senza necessità di chiamata al supporto tecnico); nel caso di momentanea dimenticanza delle credenziali, permette un veloce ripristino, evitando inutili sovraccarichi al support tecnico. Gli utilizzatori sono invitati, in caso di necessità, a provvedere in autonomia.

Continuità operativa

Le piattaforme non sono un gioco ma uno strumento, in particolar modo, di studio e di lavoro.

A volte i comportamenti superficiali o involontari possono provocare danni alle piattaforme utilizzate o ai contenuti pubblicati, impattando pesantemente sulla continuità operativa e sull'erogazione dei servizi di didattica a distanza.

La stupidità di pochi non deve poter impattare sulla maggioranza silenziosa e studiosa.

Per questo motivo si raccomanda di:

1. Avere il massimo rispetto di tutti, anche on line in piattaforma
2. Tenere comportamenti consoni, come se si fosse con la classe in aula
3. Evitare di caricare documenti estranei alle attività di studio
4. Nel caso si evidenzino dei difetti, delle vulnerabilità, degli accessi possibili anche se non dovuti, segnalare l'accaduto al proprio insegnate che provvederà ad informare il gestore della piattaforma.

A tutela di tutti, gli eventuali comportamenti non allineati o configurabili come reato ai sensi dei successivi articoli del Codice penale riportati per completezza, saranno segnalati alla Polizia Postale che provvederà a espletare le necessarie indagini. Si ricorda che sia attraverso la rete Wi-Fi libera, la connettività Internet di casa, la connessione via *tethering* oppure attraverso i sistemi di pseudo-anonimizzazione disponibili sul web, l'anonimato reale non esiste. Per la forza pubblica è sempre possibile risalire ai soggetti che hanno commesso il reato.

Articolo 640 ter Codice penale, **frode informatica**

Consiste nell'alterare un sistema informatico allo scopo di procurarsi un ingiusto profitto. La pena è quella reclusione da sei mesi a tre anni e della multa da 51 a 1.032 euro. Le cosiddette pratiche di Phishing e quelle di diffusione di appositi programmi truffaldini (Dialer) rientrano nell'ambito di applicazione di questo articolo.

Articolo 615 ter Codice penale, **Accesso abusivo ad un sistema informatico o telematico**

si sostanzia nella condotta di colui che si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo. La pena prevista è quella della reclusione fino a tre anni.

Articolo 615 quater Codice penale, **Detenzione e diffusione abusiva di codici di accesso a sistemi informatici**

Punito con la reclusione sino a un anno e con la multa sino a 5.164 euro, è commesso da chi - al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno - abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo.

Articolo 615 quinquies Codice penale, **Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema**

Punisce - con la reclusione fino a due anni e con la multa sino a euro 10.329 - la diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico. Il reato è commesso da chi si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri le apparecchiature, i dispositivi o i programmi informatici allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento.

Articolo 617 quater Codice penale e 617 quinquies Codice penale, **Intercettazione, impedimento o interruzione illecita di comunicazioni**

sanzionano rispettivamente chi, senza essere autorizzato, intercetta, impedisce, interrompe o rivela comunicazioni informatiche e colui che installa apparecchiature dirette ad intercettare, interrompere o impedire comunicazioni informatiche.

Articolo 617 sexies Codice penale, articolo 635 bis Codice penale, **Falsificazione, alterazione, soppressione di comunicazioni e danneggiamento di sistemi**

Sanzionato dal Codice penale anche chi falsifica, altera o sopprime o falsifica la comunicazione informatica acquisita mediante l'intercettazione (articolo 617 sexies c.p.) e chi distrugge, deteriora, cancella, dati, informazioni o programmi informatici (articolo 635 bis c.p.). E, con riguardo al reato di violazione e sottrazione di corrispondenza, la legge n. 547/1993, nel novellare l'articolo 616 c.p., precisa che per "corrispondenza" si intende quella epistolare, telegrafica, telefonica, informatica o telematica, ovvero effettuata con ogni altra forma di comunicazione a distanza.

Il ruolo della Polizia Postale

La Polizia Postale ha il compito di contrastare:

- la pedopornografia
- il cyberterrorismo
- la diffusione illegale di file
- la diffusione dell'hacking

Inoltre, monitora la rete Internet e conduce indagini specialistiche sull'utilizzo delle nuove tecnologie di comunicazione da parte dei gruppi antagonisti ed eversivi nazionali e stranieri. Contrasta i fenomeni della diffusione illegale di file e dell'utilizzo della rete Internet per danneggiare o per colpire, tramite la stessa, obiettivi a essa correlati. Protegge da attacchi informatici le aziende e gli enti che sostengono e garantiscono il funzionamento del Paese mediante reti e servizi informatici o telematici. Analizza ed elabora i dati relativi alle nuove frontiere del crimine informatico e si occupa dei crimini informatici legati all'e-banking e ai giochi e alle scommesse online.

Gestione di una lezione in conference call (*Netiquette Rules*)

In una lezione tramite strumenti informatici valgono le stesse regole di educazione di una lezione o riunione convenzionale frontale. Vi sono però dei vincoli e dei possibili problemi legati alle tecnologie che richiedono una particolare attenzione al fine di evitare perdite di tempo e insoddisfazione dei partecipanti.

1. È importante concordare con congruo anticipo lo strumento e il momento preciso in cui tenere la "call". L'organizzatore deve inviare un invito, verificando prima le agende condivise, in modo che sia possibile attivare semplicemente con un click lo strumento prescelto per la conferenza, senza sprechi di tempo e chiamate parallele del tipo "cosa utilizziamo per la call?";

2. considerati gli strumenti, le modalità e gli immancabili disturbi e disconnessioni, la call dovrebbe essere di una durata da 30 al massimo di 60 minuti nei quali concentrare l'essenza dei contenuti della riunione. I materiali dovrebbero essere condivisi con congruo anticipo in modo che i partecipanti possano comunque apportare il loro contributo senza discussioni o perdite di tempo; le slides per le presentazioni NON devono essere condivise preliminarmente ma mostrate esclusivamente nella sessione;
3. nel caso in cui un partecipante sappia in anticipo di un probabile ritardo, è tenuto a comunicarlo all'organizzatore in modo che, se possibile, la call venga fissata in un secondo momento o posticipata;
4. data l'impossibilità di multitasking nelle call, quando un partecipante non risponde alle chiamate o agli inviti, non è corretto insistere o lasciare messaggi, almeno la prima volta. Se dopo diversi tentativi il soggetto non risponde, è opportuno lasciare un messaggio o inviare una e-mail. A meno di particolari urgenze, l'organizzatore non dovrebbe richiamare;
5. l'organizzatore dovrebbe invitare alla call il minor numero di persone possibile poiché più persone partecipano, più difficilmente verrà prestata la dovuta attenzione;
6. tutti i partecipanti alla call devono prestare attenzione al luogo da dove viene effettuata la chiamata, ovvero in ambiente tranquillo, senza rumori di fondo e sempre supportati da una buona connettività (di solito il Wi-Fi in giardino non permette lo stesso livello di qualità audio e video); sono esclusi luoghi pubblici, in presenza di altre persone anche se familiari, specie nel caso di trattazione di temi delicati o comunque sottoposti a segreto di ufficio;
7. ad esclusione dell'organizzatore, tutti i partecipanti si accertano di tenere chiusa (in modalità *mute*) la comunicazione audio in modo da evitare rumori di fondo o effetti Larsen (feedback acustico o più ritorni); il passaggio da muto a microfono attivo è effettuato dal partecipante solo in caso di richiesta di intervento o come modalità di richiesta della parola;
8. in caso di utilizzo di sistemi di comunicazione nuovi, non conosciuti, è opportuno accertarsi preliminarmente dei prerequisiti (installazione di applicazioni software, componenti, plug-in, livelli audio) ed effettuare almeno un test preliminare;
9. nelle prime sessioni di conference è preferibile utilizzare la versione video con la ripresa delle persone sfruttando la possibilità di conoscersi se non se ne è avuta in precedenza occasione; per le versioni successive può essere consigliata la audio conference (senza video) con condivisione dei materiali; questo anche al fine di ridurre la banda di trasmissione necessaria e la qualità stessa dell'audio;
10. a meno di particolari situazioni, la call deve iniziare e concludersi nei tempi stabiliti; non è corretto attendere indefinitamente i ritardatari soprattutto per non incoraggiare la loro condotta; pertanto chi arriva in ritardo potrà essere contattato direttamente dall'organizzatore in modo da poter ricevere le informazioni perdute senza effetti negativi sugli altri partecipanti;
11. l'organizzatore della call deve mostrarsi immediatamente, presentare i partecipanti, esporre i contenuti e dare le dovute indicazioni di servizio tra le quali il tempo previsto per la call ed i relativi interventi; i partecipanti devono venire a conoscenza sin da subito di ciò che l'organizzatore si aspetta da loro;
12. la modalità di comunicazione frontale e in call si differenzia altresì per la necessità di adottare un linguaggio più semplice, frasi concise e pause regolari tra i differenti contenuti. Questo consentirà ai partecipanti di passare oltre o in alternativa di porre delle domande;
13. l'organizzatore della call deve prestare attenzione alla stessa partecipazione, intervenendo e togliendo la parola a chi prova a monopolizzare la sessione, chiamando gli altri ad intervenire;
14. pur avendo a disposizione altri strumenti del sistema informatico o lo smartphone, non è corretto continuare a rispondere alle e-mail o ai messaggi mentre gli altri partecipano attivamente alla sessione; le altre attività devono essere posticipate dopo la call;
15. prima della fine della sessione è necessario avvertire i partecipanti della imminente conclusione e della possibilità da quel momento di rivolgere opportune domande;

16. l'organizzatore della call o un soggetto nominato segretario deve annotare ed in seguito condividere il report della sessione:
    a. Motivo della call / obiettivi
    b. Nominativo e ruolo partecipanti
    c. Argomenti discussi e relativi interventi
    d. Risultanze

Allegato 1 – Applicativi e Tecniche di criptazione

Al fine di provvedere un corretto livello di sicurezza delle comunicazioni e della condivisione in piattaforme di file hosting, soprattutto se gratuite, è necessario procedere con la criptazione dei documenti soprattutto nel caso di contenuti relativi a dati personali di tipo particolare.

Per salvare un documento Word o Excel in forma criptata, utilizzare una delle seguenti modalità:

1. Salva con nome > Strumenti > Opzioni Generali > Password di lettura (2 volte);
2. File > Informazioni > Selezionare la casella Proteggi cartella di lavoro e scegliere Crittografa con password > Digitare la password;

Per criptare un documento in altro formato o un insieme di documenti, procedere con un prodotto come WinRAR:

1. Comprimere il file o la cartella in formato .zip e crittografare con metodo AES-256 (*) il file prodotto, inserendo una password di cifratura di almeno 8 caratteri;