Sistema Socio Sanitario
Regione Lombardia
ASST Nord Milano

REGOLAMENTO INFORMATICO

dell'Azienda Socio Sanitaria Territoriale Nord Milano

approvato con deliberazione del Direttore Generale
n. 753 del 04/11/2020

Principale normativa di riferimento

- Costituzione della Repubblica Italiana, art. 15

- Codice Penale, artt. 615-ter, 615-quater e 615-quinquies, 616, 617-quater, 617-quinquies, 635-bis, 635-ter, 635-quater, 635-quinquies e 640-quinquies

- Art. 4 - Legge 20 maggio 1970, n.300 “Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell’attività sindacale nei luoghi di lavoro e norme sul collocamento” (Statuto dei Lavoratori) e successive modificazioni

- D.Lgs. n.518/92 “Attuazione della direttiva 91/250/CEE relativa alla tutela giuridica dei programmi per elaboratori”

- L. n° 248/2000 “Nuove norme di tutela del diritto di autore”

- Art. 24-bis del d.Lgs. 231/2001 “Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica”

- D.Lgs. 196 del 30 giugno 2003 “Codice in materia di protezione dei dati personali” così come modificato dal D.Lgs. 101 del 10 agosto 2018

- Legge n.128 del 21.05.2004 "Conversione in legge, con modificazioni, del decreto-legge 22 marzo 2004, n. 72, recante interventi per contrastare la diffusione telematica abusiva di materiale audiovisivo, nonché a sostegno delle attività cinematografiche e dello spettacolo"

- Provvedimento del Garante per la protezione dei dati personali 1 marzo 2007 “Lavoro: Linee guida del Garante per la privacy per posta elettronica e internet” G.U. n. 58 del 10 marzo 2007 – Registro deliberazioni Del. n. 13 del 1° marzo 2007

- Legge 18 marzo 2008, n. 48 “Ratifica ed esecuzione della Convenzione del Consiglio d’Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell’ordinamento interno”

- Direttiva Dipartimento della funzione pubblica n. 02/09 del 26 maggio 2009 “Utilizzo di internet e della casella di posta elettronica istituzionale sul luogo di lavoro”

- Lettera Dipartimento per le politiche di gestione e di sviluppo delle risorse umane dell’ 8 agosto 2009 “Disciplina dell’accesso alla rete Internet”

- Linee guida in materia di Dossier sanitario - 4 giugno 2015 (G.U. n. 164 del 17 luglio 2015)

- Regolamento Europeo 2016/679 “Regolamento Generale sulla Protezione dei Dati”

- D.Lgs. 101 del 10 agosto 2018 “Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonche' alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)”

Sigle presenti nel Regolamento

Sigla	Descrizione
ASST	Azienda Socio Sanitaria Territoriale
CCE	cartella clinica elettronica
CRS	Carta Regionale dei Servizi
CUP	Centro Unico di Prenotazione
FASAS	Fascicolo socio assistenziale e sanitario
FSE	Fascicolo Sanitario Elettronico
SISS	Sistema Informativo Socio-Sanitario
UOC	Unità Operativa Complessa
UOS	Unità Operativa Semplice
SIA	Sistema Informativo Aziendale
SIC	Servizio Ingegneria Clinica
PDL	Postazioni di Lavoro
INTRANET	Accesso ai servizi informatici limitato alla sola rete aziendale
INTERNET	Accesso a servizi informatici di pubblico dominio
LAN	Rete dati locali ad un unico edificio (es presidio ospedaliero)
WAN	Rete dati geografica di intercomunicazione delle varie LAN
User id	Identificativo univoco di ogni utente
ICT	Information and Communication Technology
PC	Personal Computer

INDICE

ALLEGATI

1. PREMESSA

Le risorse tecnologiche cosiddette “ICT” (Information and Communication Technologies) costituiscono quotidianamente uno strumento di lavoro. La scarsa conoscenza dei pericoli connessi al loro uso, associata alla inadeguata cognizione delle disposizioni normative in materia di reati informatici ed alla bassa percezione del fatto che determinate azioni costituiscono spesso un reato (ossia una violazione delle norme del Codice penale vigente) – provocano in molti casi danni irreparabili. Nello specifico, un danno d’immagine, una diffamazione o un furto di “identità digitale” compiuti attraverso internet nella maggior parte dei casi non sono in alcun modo sanabili.

Per risorse tecnologiche ICT - di proprietà o comunque nella disponibilità dell’Azienda o ad essa concesse in licenza d'uso (donazioni, risorse universitarie o di proprietà delle ditte esterne) - si intende qualsiasi tipo di:

- personal computer, portatile, notebook, ecc.
- apparecchiatura biomediche che gestiscono dati,
- mezzo di comunicazione elettronica (dispositivi aziendali di fonia fissa quali telefoni fissi e fax e mobile quali cellulari, smartphone, blackberry, palmari, ecc., apparecchi di trasmissione radio quali cercapersone, walkie talkie, ecc.),
- rete di trasmissione dati,
- modem,
- stampante,
- scanner,
- apparecchiatura per l'archiviazione elettronica dei dati e relativi supporti di memorizzazione,
- macchina fotografica, videocamera e webcam,
- software operativo e programma applicativo,
- dati e informazioni in formato elettronico,
- qualsiasi altro tipo di hardware non esplicitamente menzionato.

Parlando di sicurezza delle informazioni, i parametri di riferimento da considerare sono:

- integrità, ossia la riduzione a livelli accettabili del rischio di cancellazioni o modifiche di informazioni a seguito sia di fatti accidentali e/o naturali, che di atti dolosi di soggetti non autorizzati;
- riservatezza, ossia la riduzione a livelli accettabili del rischio di accesso improprio e dell'utilizzazione dell'informazione da parte di soggetti non autorizzati;

- disponibilità, ossia la riduzione a livelli accettabili del rischio di impedimento agli utenti autorizzati di fruire del sistema informativo e di accedere e utilizzare le informazioni, sia a seguito di fatti accidentali e/o naturali che di atti dolosi di soggetti non autorizzati.

Il termine sicurezza in questo contesto indica quindi la capacità di salvaguardare la riservatezza, l'integrità e la disponibilità delle informazioni. Partendo dal presupposto che non esiste né può esistere sicurezza in modo assoluto perché i rischi non possono mai essere ridotti a zero, come sicurezza informativa si intende pertanto la capacità di prevenzione e/o reazione a minacce di tipo fisico e/o logico.

A causa dell'interconnettività e dell'interdipendenza fra le componenti di un sistema informatico, infatti, i problemi di sicurezza su una sola di esse potrebbe propagare i loro effetti, incidendo gravemente sulla sicurezza del sistema (per es. una postazione di lavoro non adeguatamente protetta può rendere vulnerabile la intranet dell'Azienda anche in presenza di firewall o altri sistemi di sicurezza perimetrale).

Premesso quindi che l'utilizzo delle risorse tecnologiche aziendali deve sempre ispirarsi al principio di necessità e correttezza, pertinenza e non eccedenza per fini determinati, espliciti e legittimi, l'ASST NORD MILANO ha adottato il presente Regolamento – che aggiorna il precedente "Disciplinare" in materia - per contribuire alla massima diffusione della cultura della sicurezza ed evitare che comportamenti inconsapevoli possano innescare problemi o danni.

Va evidenziato che il Decreto del Ministero della Funzione Pubblica 28 novembre 2000 *(Codice di comportamento dei dipendenti delle pubbliche amministrazioni)* – recentemente abrogato dal Decreto del Presidente della Repubblica 16 aprile 2013, n. 62 *(Regolamento recante codice di comportamento dei dipendenti pubblici, a norma dell'art. 54 del decreto legislativo 30 marzo 2001, n. 165)* – già forniva indicazioni in merito al comportamento che il lavoratore deve tenere in servizio; in particolare l'articolo 10, comma 3, del citato Decreto recitava testualmente: "*Il dipendente non utilizza a fini privati materiale o attrezzature di cui dispone per ragioni di ufficio. Salvo casi d'urgenza, egli non utilizza le linee telefoniche dell'ufficio per esigenze personali."*
Il principio dell'impiego dei beni del datore di lavoro per soli fini connessi alle attività istituzionali è stato perentoriamente riaffermato dall'art. 11 *(Comportamento in servizio)*, comma 3, del sopra richiamato D.P.R. 62/2013 (in vigore dal 19 giugno 2013), con il quale si è stabilito che "*Il dipendente utilizza il materiale o le attrezzature di cui dispone per ragioni di ufficio e i servizi telematici e telefonici dell'ufficio nel rispetto dei vincoli posti dall'amministrazione (…)"* .

Giova quindi precisare che le tutte risorse tecnologiche ICT dell'Azienda ospedaliera, nessuna esclusa, devono essere utilizzate esclusivamente per finalità e ragioni strettamente connesse all'attività istituzionale dell'Ente; l'uso delle stesse per fini privati non è consentito e verrà perseguito con sanzioni disciplinari e con l'avvio delle azioni civili e penali previste dall'ordinamento.

Il *Decreto Legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali"*, recentemente integrato dal D.Lgs. 101 del 10 agosto 2018, garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali nonché della dignità dei soggetti a cui si riferiscono i dati, imponendo l'adozione di misure di sicurezza che riducano il rischio informatico e consentano un efficace controllo sull'utilizzo e la conservazione dei dati.

Con il *provvedimento dell' 1 marzo 2007 "Lavoro: le linee guida del Garante per posta elettronica e internet"*, il Garante per la protezione dei dati personali ha prescritto ai datori di lavoro pubblici e privati di adottare le misure necessarie riguardanti l'onere di specificare le modalità di utilizzo della posta elettronica e della rete Internet da parte dei lavoratori, ai sensi dell'art. 154, comma 1, lett. c), del Codice in materia di protezione dei dati personali (D.Lgs. 196/2003), indicando chiaramente le modalità di utilizzo degli strumenti elettronici messi a disposizione e i relativi controlli predisponendo un disciplinare interno.

Con la *direttiva n. 02/09 "Utilizzo di internet e della casella di posta elettronica istituzionale sul luogo di lavoro"* "al fine di contemperare le esigenze di corretto ed ordinato svolgimento della vita lavorativa e di prevenzione di inutili intrusioni nella sfera personale dei lavoratori e di violazioni della segretezza della corrispondenza," **il Ministro per la Pubblica amministrazione e l'innovazione ribadisce quanto affermato dal Garante ed invita le Amministrazioni pubbliche "ad attuare tutte le misure di informazione, controllo e verifica al fine di regolamentare la fruizione delle risorse ICT e responsabilizzare i dipendenti nei confronti di eventuali utilizzi non coerenti con la prestazione lavorativa e non conformi alle norme che disciplinano il lavoro alle dipendenze delle pubbliche amministrazioni."**

La normativa in materia di protezione del software introdotta con il *D.Lgs. n.518/92 "Attuazione della direttiva 91/250/CEE relativa alla tutela giuridica dei programmi per elaboratori*" ha aggiunto l'art. 171-bis, avente ad oggetto la tutela dei programmi per elaboratori, all'art. 171 della Legge n°633/1941. L'art. 171-bis, il cui testo è stato modificato dalla *L. n° 248/2000 "Nuove norme di tutela del diritto di autore"*, prevede sanzioni penali a carico di coloro che duplicano, detengono, distribuiscono o vendono programmi per elaboratore oggetto di copyright; pertanto la norma pone il divieto assoluto di fare copie illegali di materiale protetto da leggi a tutela del diritto d'autore e di rendere tale materiale disponibile a terzi per effettuarne le copie.

La *Legge 20 maggio 1970, n.300 "Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale nei luoghi di lavoro e norme sul collocamento" (Statuto dei Lavoratori)* all'art.4 vieta di utilizzare impianti audiovisivi e altre apparecchiature per finalità di controllo a distanza dei lavoratori.

L'art. 15 della *Costituzione della Repubblica Italiana* sancisce che "La libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione sono inviolabili. La loro limitazione può avvenire soltanto per atto motivato dell'Autorità Giudiziaria con le garanzie stabilite dalla legge."

L'art. 616 del *Codice Penale* in merito di violazione, sottrazione e soppressione di corrispondenza recita "Chiunque prende cognizione del contenuto di una corrispondenza chiusa, a lui non diretta, ovvero sottrae o distrae, al fine di prendere o di farne da altri prendere cognizione, una corrispondenza chiusa o aperta, a lui non diretta, ovvero, in tutto o in parte, la distrugge o sopprime, è punito, se il fatto non è preveduto come reato da altra disposizione di legge, con la reclusione fino ad un anno e con la multa da sessanta a un milione. Se il colpevole, senza giusta causa rivela, in tutto o in parte, il contenuto della corrispondenza, è punito se dal fatto deriva nocumento ed il fatto non costituisce un più grave reato, con la reclusione fino ai tre anni. Il delitto è punibile a querela della persona offesa." Agli effetti delle disposizioni di questa sezione, per "corrispondenza" si intende quella telegrafica, epistolare, telefonica, informatica, o telematica ovvero effettuata con ogni altra forma di comunicazione a distanza.

La *legge 18 marzo 2008, n. 48 "Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento intero"* ha ampliato le fattispecie di reato che possono generare la responsabilità della aziende. L'art. 7 del provvedimento, infatti, introduce nel *D.Lgs. 231/01* l'art. 24-bis "Delitti informatici e trattamento illecito di dati" che di fatto introduce nella disciplina della responsabilità amministrativa degli enti le sanzioni per i nuovi reati informatici previsti dal Codice penale.

Il Regolamento Europeo 2016/679 apporta significative modifiche alla normativa preesistente sia in termini di adempimenti sia in termini di sanzioni. Si fonda in particolar modo sul concetto di "accountability", ossia di responsabilizzazione del Titolare e di tutti i soggetti coinvolti nel processo di trattamento dei dati personali.

La progressiva diffusione delle nuove tecnologie, ed in particolare il libero accesso alla rete Internet, espone l'Azienda ai rischi connessi ad un uso improprio o illecito degli strumenti aziendali da parte del personale. Sono intuibili, conseguentemente, i rischi per la sicurezza dei dati di proprietà dell'Ente e per il funzionamento del sistema informatico, nonché le responsabilità - sia civili, sia penali - che gravano sull'Ente qualora detti usi dovessero recare danni. L'ampia distribuzione delle risorse tecnologiche ne favorisce l'utilizzo anche per finalità diverse da quelle lavorative. L'attività di monitoraggio dell'uso improprio di tali risorse richiede un giusto bilanciamento tra l'esigenza da parte dell'Azienda di controllare che ciò non accada e il diritto alla riservatezza dei dati personali di ciascun dipendente.

E' necessario quindi essere a conoscenza dei pericoli in cui è possibile imbattersi e far rispettare le regole di comportamento dettate dall'Azienda in questo documento.

Il presente Regolamento:

- **è pubblicato sulla Intranet aziendale;**
- **è incluso nella documentazione aziendale fornita ai nuovi dipendenti da parte delle Risorse Umane;**
- **è reso noto a coloro che a diverso titolo accedono all'Azienda per motivi professionali.**

2. RESPONSABILITÀ

Il presente Regolamento aziendale, aggiornato periodicamente, è rivolto a tutto il personale - di seguito *utente* - che, a vario titolo, ha necessità di utilizzare le risorse ICT per conto dell'Azienda, nello specifico:

- ✓ dipendenti
- ✓ liberi professionisti
- ✓ specializzandi, frequentatori, borsisti, ecc.
- ✓ professionisti che – in forma individuale o attraverso altri modelli – erogano prestazioni nell'interesse dell'azienda
- ✓ tutti i soggetti - persone fisiche o giuridiche – cui l'Azienda affida, in via continuativa od occasionale, lo svolgimento di servizi di sua competenza e la cui attività è di conseguenza pienamente inserita nell'organizzazione aziendale
- ✓ altro personale autorizzato.

La gestione delle risorse aziendali è demandata al Servizio Informatico Aziendale e al Servizio di Ingegneria Clinica, per quanto di competenza. E' compito invece della Struttura di Gestione delle Risorse Umane adottare le eventuali sanzioni conseguenti ai comportamenti non conformi al presente Disciplinare.

I Dirigenti Responsabili delle singole Strutture sono tenuti ad accertarsi che gli utenti siano a conoscenza del presente documento e a vigilare sulla corretta applicazione di quanto impartito, esercitando una funzione di indirizzo e controllo e individuando con precisione le responsabilità per la gestione dei dati e delle risorse stesse.

Gli utenti sono responsabili dell'utilizzo delle risorse tecnologiche ricevute in assegnazione o poste comunque a disposizione e sono tenuti a garantirne il corretto utilizzo.

I soggetti che – a diverso titolo - utilizzano le risorse ICT devono rispettare le regole previste dal presente Regolamento e in particolare:

- mantenere una adeguata riservatezza dei dati;
- mantenere una adeguata riservatezza sulle misure di sicurezza adottate e sulle modalità di accesso ai servizi;
- utilizzare esclusivamente le risorse alla cui fruizione essi sono autorizzati per gli scopi di natura lavorativa;
- segnalare ogni accertata violazione delle norme che regolano l'utilizzazione delle risorse.

Sono possibili deroghe specificatamente autorizzate e motivate dal Servizio Informatico Aziendale o dal Servizio di Ingegneria Clinica.

Gli utenti sono tenuti a mantenersi aggiornati controllando periodicamente le direttive del SIA divulgate anche tramite e-mail e la documentazione pubblicata sulla intranet.

I fornitori esterni - ad esempio gli addetti alla manutenzione di hardware, software e reti - operano in conformità alle presenti disposizioni, sotto la sorveglianza dei Dirigenti Responsabili delle Strutture presso cui viene fornito il servizio.

3. UTILIZZO DELLE RISORSE TECNOLOGICHE ICT

Le risorse affidate agli utenti sono strumenti di lavoro. Utilizzare le apparecchiature aziendali per scopi non legati al proprio lavoro può creare danni. L'accesso alle risorse tecnologiche ICT comporta l'integrale e incondizionata accettazione delle norme del presente Regolamento e il rispetto della normativa vigente in materia.

Il computer presenta caratteristiche hardware e software impostate dal SIA, che non possono essere modificate.

Non sono consentite le seguenti operazioni:

- la modifica delle dotazioni informatiche e biomediche fornite dall'azienda aggiungendo, sostituendo o eliminando periferiche;
- qualsiasi atto che possa compromettere la sicurezza e la riservatezza delle risorse affidate;
- l'accesso, l'utilizzazione, la distruzione, l'alterazione o la disabilitazione non autorizzata di risorse ICT, anche per mezzo di chiavi di accesso (passwords, badges, ecc.) rese disponibili da altri soggetti, nonché l'abbandono senza custodia delle risorse assegnate;
- l'uso di dati o di altre risorse ICT che ecceda l'ambito lavorativo e per scopi non consentiti dalle norme vigenti;
- il danneggiamento di informazioni o programmi altrui;
- la modifica e/o la cancellazione di informazioni o programmi altrui senza opportuna autorizzazione;
- la duplicazione, l'archiviazione e l'uso di software su qualsiasi risorsa informatica in violazione a disposizioni contrattuali;
- la copia non specificatamente autorizzata di dati e informazioni;
- l'utilizzazione per scopi di interesse esclusivamente privato di qualsiasi risorsa ICT dell'azienda;
- la modifica delle caratteristiche hardware e software impostate sulle risorse assegnate, salvo previa autorizzazione esplicita da parte del SIA o del SIC;
- l'installazione di programmi e dispositivi diversi da quelli autorizzati dal SIA o del SIC;
- la riproduzione o la duplicazione di programmi informatici;
- l'installazione e/o comunque l'utilizzo di software peer-to-peer (per es. Skype, Emule, Limewire, Kazaa, Ares, BitTorrent, BitTornado, eDonkey, WinMX, Napster, Morpheus, Filetopia, SoulSeek, Shareaza, Azureus, ecc.);
- il trasferimento all'esterno dell'Azienda di file, documenti e qualsiasi altra documentazione riservata di proprietà dell'Azienda, se non per finalità strettamente attinenti allo svolgimento delle proprie mansioni e, comunque, previa autorizzazione del proprio responsabile gerarchico;

- l’uso di supporti di archiviazione removibili (es. chiavette o pen drive, dischi esterni) per la memorizzazione dei dati sensibili su postazioni che devono essere sempre funzionanti (es. pronto soccorso); negli altri casi si consiglia di adottare le necessarie precauzioni;
- installare senza autorizzazione scritta modem per l’accesso a banche dati esterne o interne all’azienda;
- svolgere attività fraudolenta di intercettazione, impedimento o interruzioni di comunicazioni relative ad un sistema informatico o telematico di soggetti pubblici o privati con i quali l’azienda intrattiene rapporti nell’ambito della propria attività, al fine di acquisire informazioni riservate;
- installare apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche;
- qualunque altra attività comunque in contrasto con il presente Regolamento aziendale o con la normativa vigente.

SPEGNIMENTO STRUMENTI INFORMATICI E APPARECCHIATURE BIOMEDICHE

Gli strumenti informatici e le apparecchiature biomediche devono essere spenti ogni sera prima di lasciare gli uffici/reparti/ambulatori (salvo diversa indicazione per esigenze di servizio), in concomitanza del cambio turno o in caso di assenze prolungate. Inoltre l’utente è tenuto a scollegarsi dal sistema ogni qualvolta sia costretto ad assentarsi dal locale nel quale è ubicata la stazione di lavoro o nel caso ritenga di non essere in grado di presidiare l’accesso alla medesima: lasciare una postazione di lavoro incustodita può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso.

Osservare le presenti disposizioni consente un risparmio energetico, sicurezza fisica del dispositivo, aggiornamenti software programmi e antivirus al successivo login.

Le postazioni che vengono utilizzate in continuo (24 ore al giorno) devono comunque essere spente e riavviate almeno una volta a settimana, per le ragioni di cui sopra. Stessa precauzione va adottata per le postazioni del personale in smartworking.

E’ necessario evitare di lasciare il PC acceso con i programmi aperti in caso di assenza (es. pausa pranzo, riunioni, ecc). In questi casi è consentito (in alternativo alla disconnessione dal PC) di attivare lo screen-saver con modalità di richiesta password alla riconnessione oppure bloccare il PC (CTR+ALT+CANC e scelta dell’opzione “blocca computer”).

Le informazioni archiviate elettronicamente devono essere esclusivamente quelle necessarie all'attività lavorativa o quelle previste dalla legge.

Costituisce buona regola la pulizia periodica (almeno ogni sei mesi) degli archivi, con la cancellazione dei file obsoleti o inutili. Questa attività comprende:

- cancellazione dei file temporanei;
- cancellazione di file non più necessari (in modo particolare nelle cartelle di rete).

È da evitarsi inoltre la duplicazione dei dati.

FURTI

In caso di smarrimento o furto di qualsiasi risorsa ICT in dotazione, occorre presentare denuncia all'Autorità Giudiziaria e informare tempestivamente il Responsabile dell'economato e, per quanto di competenza, il Responsabile del SIA o il Responsabile del SIC.

PORTATILI, ECC.

L'utente è responsabile del PC portatile assegnatogli, anche temporaneamente, dall'Azienda e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.

Ai PC portatili si applicano le regole di utilizzo previste per i PC, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna.

Per ragioni di sicurezza e di tutela della privacy, sui PC portatili non devono mai essere memorizzati dati sensibili. Utilizzare a questo scopo solo le cartelle di rete.

I PC portatili utilizzati all'esterno (convegni, visite in azienda, ecc), in caso di allontanamento, devono essere custoditi in un luogo protetto.

Inoltre, il PC portatile:

- non deve essere mai lasciato incustodito;
- deve contenere solo i file strettamente necessari;
- deve essere collegato periodicamente alla rete aziendale per consentire il caricamento dell'aggiornamento dell'antivirus;
- non deve essere utilizzato con abbonamenti internet privati per collegamenti alla rete per scopi non riconducibili ad attività istituzionali.

BANCHE DATI LOCALI

Nel caso in cui sorga la necessità di elaborare delle banche dati locali su stazioni di lavoro personali, diverse da quelle centralizzate, in formato ad esempio excel o access, la cui tutela della gestione è demandata all'utente finale, è necessario concordare preventivamente con il Sistema Informatico Aziendale le modalità operative di gestione di tali banche dati.
L'utente finale dovrà adottare le misure di sicurezza più idonee a garantire il rispetto della normativa privacy, sia sotto il profilo dell'identificazione ed autenticazione, delle modalità e della frequenza opportuna del back up e ripristino dei dati, che della disponibilità degli stessi.

BACKUP MEDIANTE SUPPORTI RIMOVIBILI

Il backup dei dati memorizzati sui server centrali è di competenza del SIA.

Nel caso in cui il salvataggio dei dati avvenga mediante l'uso di dispositivi removibili (chiavette, dischi esterni, ecc), devono essere osservate le seguenti misure di sicurezza al fine di salvaguardare la riservatezza dei dati:

- i dispositivi removibili devono essere conservati in un luogo idoneo al fine di evitare accessi non autorizzati e trattamenti non consentiti;
- i dispositivi removibili, se non utilizzati, devono essere resi inutilizzabili;
- i dispositivi removibili possono essere riutilizzati solo dopo aver provveduto a cancellare i dati e le informazioni in essi contenute; l'operazione deve essere fatta in modo che i dati precedentemente memorizzati non siano tecnicamente ed in alcun modo recuperabili. Se l'operazione non è possibile è necessario distruggere i supporti.

ADDETTI ALLA MANUTENZIONE

Gli operatori del Servizio Informatico Aziendale e del Servizio di Ingegneria Clinica, dell'Help desk affidato in outsourcing e dei fornitori esterni addetti alla manutenzione possono in qualunque momento procedere alla rimozione di ogni file o applicazione che riterranno essere pericolosi per la sicurezza su tutte le risorse ICT e alla eventuale riconfigurazione delle apparecchiature in manutenzione, anche senza preavviso.

SMALTIMENTO APPARECCHIATURE

In ottemperanza al provvedimento del Garante della privacy del 13 ottobre 2008 "Rifiuti di apparecchiature elettriche ed elettroniche (Raae) e misure di sicurezza dei dati personali", all'atto della dismissione del computer gli operatori addetti allo smaltimento provvedono a cancellare tutte le informazioni presenti sull'Hard Disk.

CESSAZIONE DEL RAPPORTO DI LAVORO O DI COLLABORAZIONE CON L'AZIENDA

In caso di cessazione del rapporto di lavoro o di collaborazione con l'ASST, l'utente non può cancellare le informazioni di interesse aziendale presenti sulle postazioni di lavoro e/o sui server, senza esplicita autorizzazione del Dirigente Responsabile della Struttura di appartenenza. Qualora l'utente abbia inavvertitamente lasciato sulle postazioni di lavoro e/o sulla rete informazioni di interesse non aziendale, le stesse verranno cancellate senza alcuna responsabilità per l'ASST.

4. UTILIZZO DELLA RETE AZIENDALE

L'accesso alla rete aziendale è riservato al personale autorizzato ed è protetto da password.

Per l'accesso deve essere utilizzato il proprio profilo personale (username e password) e le credenziali fornite dal SIA.

Il Responsabile del SIA fornisce e regolamenta l'accesso ai seguenti servizi di rete:

- ✓ assegnazione di un codice identificativo personale
- ✓ assegnazione di una password personale definita dall'utente
- ✓ accesso internet
- ✓ accesso alla Intranet aziendale
- ✓ servizio di posta elettronica con casella postale individuale ad accesso riservato e controllato da password
- ✓ casella di posta elettronica condivisa tra più lavoratori attribuita a ciascuna struttura ad accesso riservato e controllato da password, consultabile dal personale individuato dal Responsabile della Struttura di riferimento
- ✓ accesso alle aree dati istituzionali condivise tra più utenti che ne facciano richiesta motivata ed autorizzata dal Responsabile della Struttura di appartenenza
- ✓ utenza generica per accesso al sistema operativo (non agli specifici applicativi) in caso di postazioni condivisa tra più lavoratori, purché l'accesso agli specifici applicativi aziendali avvenga tramite codice identificativo personale o l'accesso al PC avvenga in locali ad accesso selezionato.

Tutti i dipendenti hanno diritto all'assegnazione di un codice identificativo personale, univoco, che non può neppure in tempi diversi essere assegnato a più utenti. Tale codice identificativo consente l'accesso alla intranet e ad una casella di posta elettronica.

Per i nuovi assunti, all'atto dell'assunzione, la Struttura Gestione delle risorse umane comunica al Responsabile del SIA i dati necessari alla creazione dell'utenza per l'accesso ai servizi di rete che, a loro volta, saranno trasmessi al Servizio di Help Desk con il compito di provvedere in merito seguendo le indicazione fornite dal Responsabile del SIA.

In caso di trasferimento interno o di cessazione, a seguito di segnalazione al SIA, verranno adottate le dovute cautele per evitare che l'utente possa continuare ad utilizzare in maniera non corretta gli strumenti aziendali e gli accessi autorizzati.

Per tutto il personale non dipendente (consulenti, specialisti ambulatoriale, frequentatori, specializzandi, collaboratori a progetto, ecc.) le operazioni di creazione, cancellazione e modifica degli account sono realizzate su specifica richiesta del Dirigente del Responsabile della struttura presso cui il suddetto personale presta servizio.

Il Responsabile del SIA, a fronte di specifiche segnalazioni, ha inoltre il compito di chiedere al Servizio di Help Desk di disattivare i codici individuali nei seguenti casi:

- ✓ personale dimesso, su indicazione dell'Ufficio del personale,
- ✓ ogni qualvolta ravvisi la perdita di qualità,
- ✓ mancato utilizzo per un periodo superiore a sei mesi.

L'Accesso agli altri servizi, su tutti l'accesso agli applicativi aziendali, è subordinato alle autorizzazioni e ai permessi attribuiti dal Responsabile del SIA a fronte di specifiche richieste formulate dal Dirigente Responsabile della Struttura presso cui l'utente presta servizio.

E' fatto divieto di:

- connettere alla rete aziendale stazioni di lavoro, portatili, stampanti, modem, ecc. se non a fronte di una esplicita e formale autorizzazione del Servizio Informatico;
- connettersi a qualunque rete wireless (WI-FI), senza previa autorizzazione del Servizio Informatico;
- utilizzare chiavette per l'accesso internet su pc/apparecchiature connessi alla rete aziendale;
- condividere cartelle in rete salvo autorizzazione del SIA;
- permettere ad altre persone l'uso del proprio account;
- monitorare ciò che transita in rete ("sniffing"), se non da parte del personale del SIA preposto alla gestione della rete e a fronte una esplicita richiesta del Responsabile del SIA a controllo e tutela delle norme indicate in questo stesso documento.

ACCESSO DA REMOTO

Relativamente alle attività di manutenzione remota su apparecchiature connesse alla rete aziendale, il personale tecnico del SIA e dell'Help Desk potrà utilizzare specifici software.
Tali programmi vengono utilizzati per assistere l'utente durante la normale attività ovvero per svolgere manutenzione su applicativi e su hardware. L'attività di assistenza e manutenzione avviene previa autorizzazione da parte dell'utente interessato. La configurazione del software prevede un indicatore visivo sul monitor dell'utente ad indicare quando il tecnico è connesso al personal computer.

Nel caso in cui si rilevi la necessità di accedere dall'esterno alle risorse riservate alla rete interna aziendale (ad esempio: fornitori degli applicativi, fornitori di servizi di rete, addetti alla manutenzione di apparecchiature biomediche, medici reperibili, medici in libera professione presso studi privati, ecc.), il Dirigente Responsabile della struttura di riferimento del personale che deve accedere da remoto alle risorse aziendali effettua una formale richiesta al Responsabile del SIA. Questi, verificato che esista tra il soggetto e ASST Nord Milano un adeguato accordo in tema di privacy, può autorizzare un accesso da remoto alle risorse interne necessarie per lo svolgimento delle attività – che possono variare caso per caso - mediante un collegamento tramite VPN (Virtual Private Network). Tipicamente l'accesso VPN consente ad un utilizzatore di connettersi da un'azienda esterna o da casa via ADSL con il proprio operatore e di collegarsi ai servizi di rete aziendali come se si trovasse all'interno della rete.
Gli accessi remoti o tramite VPN vengono tracciati attraverso appositi strumenti di monitoraggio e reportistica al fine di poter avere un quadro aggiornato in qualsiasi momento si renda necessario.

Gli utenti che si avvalgono dell'accesso da remoto devono attenersi alle disposizioni del presente Regolamento garantendo la riservatezza dei dati che vengono trattati all'esterno dell'Azienda.

Sono garantite le misure di sicurezza previste dalle vigenti norme in tema di riservatezza dei dati personali.

5. GESTIONE DELLE CREDENZIALI DI ACCESSO (USERID E PASSWORD)

Le password di accesso alle risorse tecnologiche ICT dotazioni informatiche, alle apparecchiature biomediche, alla posta elettronica, ai vari programmi in rete e – in ogni caso – a tutte le risorse tecnologiche aziendali - sono attribuite dal Servizio Help Desk, su indicazione del SIA. Fanno eccezione i sistemi di cui il personale aziendale non è Amministratore di sistema (ad esempio i PIN delle carte SISS, il sistema di prescrizione delle protesica, ecc).

L'utente è tenuto a:

- cambiare la propria password al primo utilizzo e, successivamente, ogni 3 mesi;
- non riutilizzare le ultime due password utilizzate;
- utilizzare password lunghe almeno otto caratteri, che contengano lettere, maiuscole e minuscole, numeri e caratteri speciali (es.: * # @ ? !);
- non usare password che contengano riferimenti personali che possano ricondurre facilmente all'utente (nome di battesimo, data di nascita, nome del coniuge o dei figli, ecc.);
- conservare nella massima segretezza la parola di accesso e qualsiasi altra informazione legata al processo di autenticazione;
- sostituire la password nel caso si sospetti che la stessa abbia perso la segretezza;
- non utilizzare la medesima password su sistemi differenti.

Nel caso in cui l'utente ravveda gli estremi per richiedere il reset della propria password (dimenticanza, perdita della sicurezza, ecc.) è necessario inoltrare richiesta scritta all'Help desk – anche via mail – in modo tale da garantire le generalità del richiedente.

Qualora l'utente sia assente e risulti necessario accedere ai dati di sua pertinenza, il Responsabile della struttura a cui appartiene l'utente può palesare la problematica al Responsabile del SIA il quale, se ritiene che non esistano altre modalità di accesso ai dati, può effettuare il reset della password dell'utente avvisandolo al suo rientro di quanto accaduto. L'utente dovrà quindi modificare la sua password al primo accesso.

Verranno rispettate tutte le misure di sicurezza previste dalle vigenti norme in materia di privacy.

6. USO DELLA SMARTCARD SISS

Il Titolare della Carta a Microprocessore (smartcard) deve gestire la stessa con diligenza, evitando le situazioni in cui possa perderne il controllo (es. lasciare la Carta incustodita). Tale carta consente l'accesso ad informazioni amministrative e sanitarie anche al di fuori dei sistemi aziendali.
L'operatore Titolare di carta deve modificare al primo accesso, nei casi in cui ne ritenga compromessa la confidenzialità e in ogni caso ogni tre mesi il codice PIN (Personal Identification Number) Utente necessario per il processo di autenticazione per l'accesso ai servizi SISS e il PIN Firma necessario per la firma elettronica, se abilitata.

I codici di accesso (PIN/PUK) alle funzioni di autenticazione e firma sono strettamente personali, non devono assolutamente essere comunicati ad altri e occorre evitare di trascriverli in chiaro, su carta o su altro supporto informatico.
I codici di accesso (PIN) devono avere una lunghezza di 8 caratteri; nella scelta dei caratteri si consiglia di seguire le seguenti regole (derivate da statistiche specifiche):

- i PIN devono essere costituiti utilizzando caratteri alfabetici e/o numerici;
- i PIN non devono contenere caratteri di spaziatura;
- i PIN non devono contenere parole facilmente riconducibili all'operatore (per esempio i dati anagrafici, data di nascita, suoi o dei suoi familiari, numero di matricola dell'operatore, nomi di propri animali domestici).
- i due codici di accesso (PIN di identificazione e PIN di firma) non devono essere creati identici.

In particolare per le carte In particolare per le carte operatore SISS con diritti di firma digitale (es: carte operatore per ruolo medico), dal momento che consentono la firma di documenti legalmente validi anche al di fuori del servizio sanitario regionale (es: scritture private) si raccomanda una cura particolare, anche per evitare spiacevoli conseguenze personali. Lo stesso vale per qualunque dispositivo di firma digitale.
Dal momento che la firma digitale ha una scadenza, per tutti quei documenti firmati gestiti al di fuori degli ordinari applicativi aziendali si raccomanda di concordare con il SIA gli eventuali processi di marcatura temporale e conservazione legale sostitutiva.
Il Titolare di Carta deve archiviare in modo sicuro i due codici PUK (Pin Unblocking Key), con i quali gli è possibile sbloccare la smartcard dopo il ripetuto (3 volte) inserimento errato del PIN.
In caso di perdita o furto della smartcard o di compromissione dei codici PIN/PUK, il Titolare della smartcard deve rivolgersi tempestivamente al Punto di Adesione/Punto di Registrazione (PdA/PdR) presso l'Ufficio del Personale dell'Azienda.
In caso di trasferimento del Titolare ad altra Azienda sanitaria, la Carta rimane in possesso del Titolare. Nel caso invece di cessazione del rapporto (ad esempio pensionamento o trasferimento ad azienda non sanitaria), il Titolare deve restituire la Carta recandosi presso il PdA/PdR.

7. INTERNET/INTRANET E I RELATIVI SERVIZI

La rete internet è una risorsa messa a disposizione degli utenti come fonte di informazione per finalità di documentazione, ricerca e studio, utili per lo svolgimento delle mansioni assegnate. Quindi l'utilizzo di Internet deve essere limitato a scopi inerenti l'attività lavorativa.

Al fine di ridurre il rischio di usi impropri della "navigazione" in internet mediante l'utilizzo degli strumenti abilitati (pc, portatili, dispositivi mobili, ecc) – ad esempio attività non correlate con la prestazione lavorativa quali la visione di siti non pertinenti o con finalità ludiche – l'ASST ha adottato opportune misure che possono prevenire eventuali controlli successivi sul lavoratore:

- individuazione di categorie di siti considerati attinenti o meno con l'ambito lavorativo;
- configurazione dei sistemi e utilizzo di filtri allo scopo di prevenire determinate operazioni ritenute incoerenti con l'attività lavorativa quali l'upload o l'accesso a determinati siti inseriti in una blacklist e/o il download di file o software aventi particolari caratteristiche - dimensionali o di tipologia di dato;
- trattamento dei dati in forma anonima o tale da precludere l'immediata identificazione di utenti mediante opportune aggregazioni (ad esempio i file di log riferiti al traffico web, su base collettiva o per gruppi sufficientemente ampi di utenti);
- conservazione dei dati per il tempo strettamente necessario al perseguimento di finalità organizzative, produttive e di sicurezza.

Nel corso della navigazione l'utente è tenuto a leggere con attenzione qualsiasi finestra, pop up, o avvertenza prima di proseguire nella navigazione e soprattutto prima di accettare eventuali condizioni contrattuali o di aderire alle iniziative proposte online.

E' fatto espresso divieto di adottare comportamenti non pertinenti all'attività istituzionale come di seguito dettagliato:

- è vietato modificare le impostazioni del web browser (explorer, firefox, ecc);
- non è permesso il download di software, di file musicali o video. Ciò, infatti, potrebbe inconsapevolmente esporre a rischi di un coinvolgimento sia patrimoniale che penale, creando problemi alla sicurezza e all'immagine dell'Azienda stessa;
- è fatto divieto all'utente di visitare siti illegali o che possano costituire un pericolo per la sicurezza aziendale (siti per adulti – siti di suonerie, sfondi per cellulari ecc.);

- non possono essere utilizzati modem privati, chiavette o altri dispositivi per il collegamento alla rete internet;
- è vietata ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa, la partecipazione a forum non professionali, l'utilizzo di chat-line e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames);
- è vietato pubblicare foto o altri documenti aziendali senza opportuna autorizzazione;
- è vietato accedere a testi, immagini o animazioni lesive della pubblica decenza;
- è vietato implementare siti internet pubblicando informazioni aziendali senza opportuna autorizzazione;
- non sono consentiti l'accesso e la memorizzazione di documenti informatici di natura oltraggiose e discriminatorie per sesso, lingua, religione, origine etnica, opinioni politiche o sindacali.

Nel caso in cui si presentasse l'esigenza di accedere a siti che risultano bloccati, l'utente provvede a richiedere il supporto tecnico all'Help desk che attiverà gli opportuni canali di verifica per l'eventuale autorizzazione.

Per monitorare il corretto funzionamento del portale (internet/intranet) vengono raccolti dati inerenti l'operazione effettuata, l'indirizzo IP, il nome dell'utente (solo in caso di accesso alla intranet), data e ora in cui è avvenuto l'accesso. I dati raccolti non vengono comunicati a terzi e vengono conservati per il periodo minimo richiesto dalla normativa vigente. Tali dati potrebbero essere utilizzati per l'accertamento di responsabilità in caso di eventuali reati informatici (ad esempio pubblicazione o cancellazione impropria di dati).

Durante la navigazione sul portale non viene fatto uso di cookies per le informazioni di carattere personale, né vengono utilizzati cookies persistenti di alcun tipo ovvero sistemi per il tracciamento utenti. L'uso dei cookies di sessione (che non vengono memorizzati in modo persistente sul computer dell'utente e svaniscono con la chiusura del browser) è strettamente limitato alla trasmissione di identificativi di sessione necessari per consentire l'esplorazione sicura ed efficiente del sito ed evitano il ricorso ad altre tecniche informatiche potenzialmente pregiudizievoli per la riservatezza della navigazione degli utenti e non consentono l'acquisizione di dati personali identificativi dell'utente. Nessun dato derivante dal servizio web viene comunicato o diffuso, salvo nei casi espressamente previsti dalla legge.

8. USO DELLA POSTA ELETTRONICA

La posta elettronica è uno strumento di proprietà aziendale messo a disposizione esclusivamente per motivi di lavoro; di conseguenza deve essere utilizzato in tale ambito, nel rispetto degli obblighi derivanti dalle norme di legge e contrattuali che disciplinano il rapporto di lavoro.

Di norma si può accedere alla posta elettronica utilizzando ZIMBRA nei seguenti modi:

- all'interno dell'azienda, dalla intranet,
- all'esterno dell'azienda, dal portale aziendale. Eventuali casi particolari possono essere analizzati dal SIA.

Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse e devono mantenerle in ordine, cancellando documenti inutili e soprattutto allegati ingombranti. Si raccomanda di cancellare periodicamente le mail inviate che non è necessario conservare e il cestino con le mail eliminate.

L'utente che si assenta per lunghi periodi (ad esempio ferie) deve provvedere ad attivare l'opzione **"Fuori sede"** in cui indicare chi contattare in sua assenza.

In caso di cessazione del rapporto di lavoro o di collaborazione con l'ASST, la casella di posta elettronica individuale sarà mantenuta attiva per il tempo strettamente necessario a gestire il passaggio di consegne.

COMPORTAMENTI CORRETTI

Ne consegue che gli utenti devono adottare comportamenti adeguati evitando quelli scorretti, come di seguito specificato:

- nel caso di mittenti sconosciuti e/o messaggi insoliti, cancellare i messaggi senza aprirli per non correre il rischio di essere infettati da virus;
- non cliccare su link contenuti all'interno di mail a meno di comprovata sicurezza sul contenuto dei siti richiamati;
- non fornire le proprie credenziali (account e/o password) e – in genere - tutti i propri dati personali se la richiesta arriva tramite una mail di dubbia provenienza e informare immediatamente il Servizio Informatico Aziendale;
- non aprire messaggi che contengono allegati sospetti (file con estensione .exe .scr .pif .bat .cmd) e successiva esecuzione delle macro in esso contenute, anche provenienti da mittenti conosciuti;

- nel caso in cui si debba inviare un documento all'esterno dell' Azienda, utilizzare preferibilmente un formato protetto da scrittura (ad esempio il formato Acrobat *.pdf). Tale software specifico è fornito dal SIA e può essere installato dagli addetti del Servizio Help Desk previa richiesta;
- non è consentito utilizzare la posta elettronica per motivi non attinenti allo svolgimento delle mansioni assegnate;
- è vietato utilizzare tecniche di "mail spamming" cioè di invio massiccio di comunicazioni a liste di distribuzione aziendali, extra aziendali o di azioni equivalenti;
- non è consentito l'utilizzo dell'indirizzo di posta elettronica istituzionale per la partecipazione a dibattiti, forum, mailing-list e/o form, salvo specifica autorizzazione in tal senso da parte del Responsabile;
- è vietato utilizzare il servizio di posta elettronica per inoltrare giochi, scherzi, barzellette, appelli e petizioni (anche se possono sembrare veritieri e socialmente utili), messaggi tipo "catene di S. Antonio" e altre e-mail che non siano di lavoro (messaggi a diffusione capillare e moltiplicata) in quanto possono limitare l'efficienza del sistema di posta.;
- è vietato allegare al testo delle comunicazioni materiale potenzialmente insicuro (ad es. programmi, scripts, macro), così come file di dimensioni eccessive. In quest'ultimo caso è preferibile usare i formati compressi (*.zip, *.rar, *.jpg);
- è vietato utilizzare indirizzi mail non aziendali per trasmettere messaggi connessi alla propria attività istituzionale;
- nel caso di documenti acquisiti tramite scanner, assicurarsi di settare la modalità di acquisizione in bianco/nero o scala di grigi. Utilizzare il colore solo se strettamente necessario: le dimensioni del file acquisito cambiano drasticamente.

  Ridurre le dimensioni dei file applicando preventivamente procedure di compressione (file zip).

INVIO MAIL CONTENENTI DATI PERSONALI SENSIBILI E/O GIUDIZIARI

E' vietato trasmettere mail che contengano dati personali, sensibili e/o giudiziari (ad esempio nome e cognome di un paziente e relativa diagnosi). Nei casi in cui sia invece strettamente necessario per la salvaguardia dell'incolumità della persona, nel rispetto delle norme per la protezione dei dati personali, occorre seguire le seguenti modalità:

- inviare il file in allegato (e non come corpo della email);
- utilizzare opportune tecniche di cifratura, avvalendosi di strumenti preventivamente concordati con il Sistema Informatico Aziendale.

CCN (COPIA CONOSCENZA NASCOSTA)

L'Azienda invita ad un uso appropriato della modalità di invio dei messaggi di posta elettronica a destinatari in copia conoscenza nascosta (Ccn), detta anche copia carbone nascosta, traduzione dell'inglese blind carbon copy (Bcc). I destinatari specificati nel campo Ccn ricevono una copia del messaggio inviato, ma il loro indirizzo viene nascosto agli altri destinatari del messaggio (inclusi altri destinatari in Ccn). Usando il campo Ccn è quindi possibile inviare il messaggio contemporaneamente a tutti i destinatari senza rivelare a nessuno di essi gli altri destinatari e i loro indirizzi.

Il Ccn si configura quale strumento di fondamentale importanza per la protezione della privacy e la lotta allo spamming nel caso di messaggi di posta elettronica inviati non solo ad un insieme di destinatari estranei fra loro, come ai sottoscrittori di una newsletter o di una mailing list, ma, ad esempio, anche ai destinatari delle catene di sant'Antonio.

Il mancato uso di tale elementare meccanismo di protezione della privacy nelle e-mail di massa comporta invece situazioni spiacevoli:

- la creazione involontaria di lunghi elenchi di indirizzi email che, accumulatisi inoltro dopo inoltro, vengono spesso intercettati dagli spammer che li utilizzano poi per inviare e-mail indesiderate di varia natura (pubblicità e malware in particolare);
- l'invio di messaggi che contengono dati personali o riferimenti a dati personali relativi ai destinatari (nel corpo del testo o solamente nell'oggetto della mail) diffondendoli a tutti i destinatari presenti nella lista rappresenta un trattamento illecito di dati;
- l'uso frequente dei sistemi di spam del campo Ccn in modi ingannevoli, per esempio per far credere a chi riceve il messaggio di essere l'unico destinatario, oppure di non essere affatto il destinatario del messaggio e di averlo ricevuto per errore.

Vi è anche un utilizzo del campo Ccn che può essere interpretato come fraudolento o lesivo della privacy, quando questo strumento sia utilizzato come espediente per rendere visibili a terzi uno scambio epistolare, all'insaputa di almeno uno dei mittenti. L'Azienda invita a non usare questa modalità per non incorrere in una eventuale sanzione disciplinare.

INOLTRO MAIL

L'inoltro di una mail "riservata", o che contiene informazioni a carattere confidenziale da parte del mittente – anche se inerenti l'attività istituzionale - ad un altro destinatario senza il consenso dell'autore costituisce una violazione della privacy. Secondo l'art. 93 della legge sui diritti d'autore – norma strettamente connessa alla privacy - la trasmissione verso terzi (attraverso l'inoltro) di un messaggio di posta elettronica, senza il consenso dell'autore, è contraria al diritto d'autore. Il consenso alla pubblicazione da parte dell'autore non deve essere necessariamente scritto o espresso, ma può risultare anche da comportamenti concludenti, in forma implicita.

Bisogna tuttavia distinguere tra:

- il reply (rispondi/rispondi a tutti): ossia quando il ricevente della mail risponde al mittente. In tal caso non può esserci lesione del diritto d'autore, in quanto l'opera torna al proprio creatore.
- il forward (inoltro): quando la mail viene inoltrata a soggetti diversi dall'autore. In questa ipotesi, la trasmissione del testo contenuto nel messaggio originale, se non autorizzata dall'autore, può integrare due diversi e concorrenti illeciti:

  a. la violazione del diritto d'autore dell'autore della mail, solo se il contenuto della mail è di carattere creativo e originale

  b. la violazione della privacy dell'autore dell'email: anche se il contenuto della mail è di carattere creativo, purché il contenuto riguardi fatti relativi alla sfera privata dell'autore.

SPAMMING

Per spamming s'intende l'invio di messaggi indesiderati, soprattutto commerciali, ma non solo. Può essere attuato attraverso qualunque sistema di comunicazione - ma il più usato è internet - attraverso messaggi di posta elettronica, chat o forum. L'Azienda ha protetto il server di posta elettronica con un filtro antispamming che impedisce la ricezione di messaggi impropri analizzando le forme e il contenuto di ogni singolo messaggio. Dal momento che questo potrebbe determinare la perdita di alcuni messaggi che non sono reale spam, il filtro è stato configurato, con metodi euristici, in modo da minimizzare il rischio di "falsi positivi" accettando d'altro canto la possibilità di ricevere qualche "falso negativo".

Il Garante della privacy ha intrapreso una campagna informativa con l'obiettivo di fornire indicazioni utili per prevenire e contrastare la ricezione di messaggi commerciali indesiderati, se non addirittura molesti. Il documento predisposto, allegato al presente Regolamento, descrive in forma sintetica le principali cautele da adottare per un uso più consapevole della posta elettronica, ma anche di altri sistemi di comunicazione personale (telefono, sms, whatsapp, social network), e per evitare anche involontarie diffusioni dei propri dati personali.

9. PROTEZIONE ANTIVIRUS, SALVATAGGIO E SMALTIMENTO

La continua diffusione di malware, cioè qualsiasi software creato con il solo scopo di causare danni più o meno gravi ad un computer o un sistema informatico su cui viene eseguito, comporta l'adozione da parte dell'Azienda di misure stringenti per tutelare le risorse informatiche, il patrimonio informativo aziendale e naturalmente i dati personali.

Ogni strumento informatico è stato pertanto dotato di software antivirus - programmato per essere aggiornato ogni quattro ore. Gli utenti devono in ogni caso tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico aziendale.

Nel caso in cui il software antivirus rilevi la presenza di un virus che non è riuscito a ripulire, l' utente dovrà immediatamente sospendere ogni elaborazione in corso senza spegnere il computer e segnalare l'accaduto all'Help Desk o al SIA.

Ogni dispositivo mobile di memorizzazione (cd, dvd, chiavette, schede sd, ecc.) di provenienza esterna all'azienda - prima del suo utilizzo - dovrà essere verificato mediante il programma antivirus in dotazione sulle postazioni di lavoro e, nel caso venga rilevato un virus non eliminabile dal software, il dispositivo non dovrà essere utilizzato.

Nel caso particolare di dati relativi all'identità genetica, questi sono trattati esclusivamente all'interno di locali protetti accessibili ai soli autorizzati ai trattamenti ed ai soggetti specificatamente autorizzati ad accedervi. Il trasporto dei dati all'esterno dei locali riservati al loro trattamento deve avvenire in contenitori muniti di serratura o dispositivi equipollenti.

Per l'archiviazione file con dati personali e/o sensibili: evitare il salvataggio sui dischi locale del PC e utilizzare in alternativa le cartelle di rete, appositamente predisposte dal SIA. Si rammenta infatti che il contenuto delle cartelle di rete viene sottoposto a backup giornaliero e con profondità storica di 1 mese e che l'accesso a queste cartelle è governato da politiche di sicurezza che ne permettono l'utilizzo solo al personale autorizzato.
Quanto conservato in locale sui PC è sotto la completa responsabilità degli utilizzatori, sia per quanto attiene la disponibilità del dato (in caso di rottura del PC), sia per gli aspetti di tutela della privacy (accesso non controllato da parte di terzi).
Si evidenzia che non è consentita la memorizzazione di dati sensibili su supporti rimovibili (e in quanto tali soggetti a smarrimento o facilmente asportabili dal proprio luogo di lavoro). In caso di necessità e previa autorizzazione del Responsabile del SIA, è possibile effettuare una copia adottando però opportune tecniche di cifratura dei dati, tali da renderli non intellegibili nel caso di smarrimento o furto.
È altrettanto vietato dalle disposizioni vigenti l'invio di dati sensibili via mail a meno che vengano utilizzate adeguate tecniche di cifratura dei dati.

Tutti i supporti di archiviazione da smaltire sono assimilati a “rifiuti speciali” e in quanto tali devono essere gestiti secondo procedure specifiche al fine di assicurare che il contenuto non possa essere in nessun modo acceduto da terzi. Per le procedure di smaltimento occorre contattare la Direzione Medica di presidio, competente per queste attività.

I supporti sopra citati possono essere riutilizzati da altri soggetti se le informazioni precedentemente in essi contenute non sono intelligibili né tecnicamente in alcun modo ricostruibili (ad esempio mediante formattazione a basso livello).

10. DISPOSITIVI DI FONIA FISSA E MOBILE E APPARECCHI DI TRASMISSIONE RADIO

I dispositivi di fonia fissa (telefoni fissi e fax) e mobile (cellulari, smartphone, palmari, ecc) e gli apparecchi di trasmissione radio (cercapersone, walkie talkie, ecc.) che l'ASST mette a disposizione - su richiesta motivata da parte del Responsabile della struttura di appartenenza del personale richiedente - devono essere utilizzati in modo strettamente pertinente allo svolgimento dell'attività lavorativa, secondo un utilizzo appropriato, efficiente, corretto e razionale.

L'assegnatario dei sopracitati dispositivi è responsabile del loro utilizzo e della loro custodia. Le conversazioni che vengono effettuate devono rispettare i principi dettati dal Codice privacy in modo da evitare che persone non autorizzate possano venire a conoscenza di informazioni riservate con riferimenti a dati personali e/o sensibili di soggetti terzi.

Solo in caso di particolare necessità e/o urgenza, i dispositivi possono essere utilizzati per motivi non attinenti l'attività lavorativa e, comunque, non in modo ripetuto o per periodi di tempo prolungati. Per comunicazioni a carattere privato, è quindi preferibile, laddove possibile, utilizzare i telefoni cellulari personali. Per l'eventuale uso promiscuo (anche per fini personali) dei dispositivi mobili occorre chiedere di attivare il sistema della "doppia fatturazione" o "dual billing", mediante il quale il costo delle comunicazioni e dei messaggi viene addebitato direttamente sul conto corrente del Dipendente.

Al fine di consentire il monitoraggio dei costi delle linee telefoniche, l'Azienda:

- tiene traccia delle chiamate entranti e uscenti da ogni telefono fisso interno;
- riceve dal fornitore delle linee mobili il report delle chiamate entranti/uscenti associate ad ogni SIM;
- predispone dei report ai fini del monitoraggio dei costi.

In caso di anomalie riscontrate nelle modalità di utilizzo dei dispositivi assegnati, si applicherà quanto previsto dal presente disciplinare nella sessione dedicata ai controlli e alle sanzioni disciplinari.

11. CONTROLLI E SANZIONI DISCIPLINARI

Il Titolare del trattamento garantisce che il trattamento dei dati personali dei dipendenti, effettuato per verificare il corretto utilizzo delle risorse tecnologiche ICT, 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;
2. il principio di correttezza, secondo cui le caratteristiche essenziali dei trattamenti devono essere rese note ai lavoratori 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;
3. il principio di pertinenza e non eccedenza, in virtù del quale:
   - i trattamenti devono essere effettuati per finalità determinate, esplicite e legittime;
   - il datore di lavoro deve trattare i dati "nella misura meno invasiva possibile" e seguire il principio di minimizzazione dei dati;
   - le attività di monitoraggio devono essere svolte solo da soggetti preposti e essere mirate sull'area di rischio, tenendo conto della normativa in materia di protezione dei dati personali e, se pertinente, del principio di segretezza della corrispondenza.

L'Azienda si riserva la facoltà di verificare a livello informatico, per finalità di sicurezza e tutela del proprio patrimonio, l'esistenza di un comportamento illecito del dipendente nell'uso degli strumenti elettronici, accesso a internet e uso della posta elettronica.

Le verifiche si svolgeranno nel rispetto della libertà, della segretezza delle comunicazioni e delle garanzie previste dallo Statuto dei lavoratori e dal Codice Privacy. In particolare, sarà possibile verificare gli accessi a Internet e i tempi di connessione senza indagare sui siti oggetto di accesso, in ottemperanza a quanto previsto dal Garante Privacy, salvo esplicita richiesta da parte dell'Autorità Giudiziaria.

A seguito delle verifiche informatiche potranno essere raccolti dati personali che saranno trattati in modo lecito e secondo correttezza, nel rispetto dei principi di pertinenza e non eccedenza della finalità di tutela della sicurezza e del patrimonio.

Eventuali informazioni di natura sensibile potranno essere trattate dall'Azienda se necessario per far valere o difendere un diritto in sede giudiziaria.

L'Azienda si è dotata di uno strumento di controllo e monitoraggio del traffico internet con registrazione degli accessi effettuati da ogni postazione / utente. Queste registrazioni possono essere utilizzate nel caso di indagini o su richiesta dell'Autorità Giudiziaria.

I log del traffico internet vengono utilizzati per produrre report statistici sulla natura degli accessi (es. siti più acceduti, tempi di connessione, volumi di traffico effettuati) in forma anonimizzata ai fine di una corretta gestione della sicurezza e dell'utilizzo appropriato degli strumenti messi a disposizione dell'utenza.

L’Azienda non effettua in alcun caso trattamenti di dati personali mediante sistemi hardware e software che mirino 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 del personale 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 dall’utente;
- 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 degli utenti.

12. GESTIONE DEI LOG

Alcune attività dell'utenza sono però soggette a logging per ragioni di sicurezza; ciò significa che alcune operazioni eseguite dagli utenti possono essere memorizzate in formato elettronico e conservate per un certo periodo di tempo.

Log in inglese significa tronco di legno; nel gergo nautico del 1700 era il pezzo di legno fissato ad una fune con nodi a distanza regolare, lanciato in mare e lasciato galleggiare. Il numero di nodi fuori bordo, entro un intervallo fisso di tempo, indicava approssimativamente la velocità della nave. Nel 1800 il logbook era il registro di navigazione su cui venivano segnati gli eventi in ordine cronologico ad intervalli regolari quali la velocità, il tempo, la forza del vento, oltre a eventi significativi che accadevano durante la navigazione.
Con il significato di giornale di bordo, nel 1963 il termine *log* è stato importato nell'informatica per indicare:

- la registrazione cronologica delle operazioni man mano che vengono eseguite;
- il file su cui tali registrazioni sono memorizzate.

Di seguito vengono dettagliate le tipologie di log raccolti e conservati:

- log della navigazione web, del firewall e del server di posta per poter effettuare verifiche di sicurezza e poter identificare anche a posteriori incidenti di sicurezza, violazione delle policy o attività fraudolente e procedere alla raccolta delle evidenze;
- log degli accessi degli amministratori di sistema ai sistemi amministrati in ottemperanza al Provvedimento del Garante per la Protezione dei dati personali relativo agli amministratori di sistema;
- log degli accessi degli utenti ai servizi di rete per poter effettuare verifiche di sicurezza e poter identificare anche a posteriori incidenti di sicurezza, violazione delle policy o attività fraudolente e procedere alla raccolta delle evidenze;
- log delle attività svolte da utenti e amministratori di sistema nell'ambito di alcuni software complessi per poter individuare anche a posteriori eventuali violazione delle policy e audit sulla correttezza dei dati gestiti dal software stesso;
- log delle operazioni ritenute rilevanti effettuate sulle base dati mediante l'utilizzo degli applicativi aziendali (Hopera, Elefante, Concerto, ecc.).

L'ASST utilizza i log delle operazioni rilevanti effettuate sulle base dati mediante l'utilizzo degli applicativi aziendali per compiere le seguenti attività, nel rispetto della normativa vigente:

- analisi delle segnalazioni di errore,
- produzione di statistiche di esercizio,
- ripristino di situazioni precedenti,
- analisi delle modifiche fatte alla base dati,
- analisi delle operazioni fatte e responsabili di tali operazioni,
- riassunto di quanto successo in un determinato arco di tempo.

Il periodo di conservazione di questi log è necessariamente illimitato.

Per tutte le altre tipologie di log il tempo di conservazione è fissato ad un periodo di un anno per consentire la verifica delle attività degli amministratori di sistema prevista dal provvedimento del Garante per la Protezione dei dati personali relativo agli amministratori di sistema e di avere una policy di retention dei log uniforme, in modo da semplificare ed economizzare la gestione del sistema dei log e delle politiche di backup.

L'ASST effettua controlli a campione, in conformità alla legge, per accertare il corretto e lecito uso di Internet e della posta elettronica e per assicurare la funzionalità e sicurezza del sistema informatico.

Le modalità del controllo sono di seguito definite:

- una prima verifica viene effettuata su dati aggregati, riferiti all'intera azienda o su aree specifiche, in relazione alla tipologia di controllo da attuare;
- in conclusione del controllo anonimo viene emesso un avviso generalizzato relativo ad un eventuale utilizzo anomalo degli strumenti aziendali e con l'invito ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite. L'avviso potrebbe essere circoscritto ad utenti afferenti all'area, presidio o struttura in cui è stata rilevata l'anomalia;
- in presenza di successive anomalie, si procederà ad effettuare controlli su base individuale, nel rispetto delle prescrizioni del Codice in materia di protezione dei dati personali.

Con la stessa gradualità vengono effettuati controlli sull'occupazione dello spazio di memorizzazione sui server aziendali attraverso le seguenti fasi:

- analisi aggregata dei dati memorizzati sui server a livello di intera struttura lavorativa (reparto, servizio, ecc.) e rilevazione della tipologia di utilizzo (file audio, file video, immagini, software non autorizzato) e relativa pertinenza con l'attività lavorativa;

- emanazione di un avviso generalizzato relativo ad un riscontrato utilizzo anomalo degli strumenti aziendali, con l'invito ad attenersi scrupolosamente ai compiti assegnati ed alle istruzioni impartite; il richiamo all'osservanza delle regole può essere circoscritto agli operatori afferenti il settore in cui è stata rilevata l'anomalia;
- in caso di successivo permanere di una situazione non conforme, è possibile procedere con un analisi puntuale ed una eventuale eliminazione del materiale non conforme anche sulle singole postazioni di lavoro.

Il monitoraggio delle soglie di allarme è sempre attivo ma i controlli normalmente non sono prolungati, costanti o indiscriminati.

I sistemi informatici e le procedure software preposte al funzionamento del portale aziendale (Internet/Intranet) acquisiscono, nel corso del loro normale esercizio, alcuni dati personali relativi a persone identificate o identificabili, la cui trasmissione è implicita nell'uso dei protocolli di comunicazione di internet. In questa categoria di dati rientrano gli indirizzi IP, l'eventuale nome del file ottenuto in risposta ed altri parametri relativi al sistema operativo e all'ambiente informatico dell'utente. Questi dati vengono utilizzati fine di ricavare informazioni statistiche anonime sull'uso del portale e per controllare il corretto funzionamento e vengono mantenuti per il periodo minimo richiesto dalla normativa vigente. Per lo stesso scopo, durante la consultazione della intranet vengono anche raccolti l'identificativo dell'utente che ha navigato, il tipo di operazione effettuata e ora/data dell'operazione. Tali dati potrebbero essere utilizzati per l'accertamento di responsabilità in caso di eventuali reati informatici ai danni del sito.

I sistemi software sono stati configurati in modo da cancellare periodicamente ed automaticamente (attraverso procedure di sovraregistrazione come, ad esempio, la rotazione dei CD contenenti i log file) i dati personali relativi agli accessi ad Internet e al traffico telematico, la cui conservazione non sia necessaria. In assenza di particolari esigenze tecniche o di sicurezza, la conservazione temporanea dei dati relativi all'uso degli strumenti elettronici è giustificata da una finalità specifica e comprovata e limitata al tempo necessario.

Un eventuale prolungamento dei tempi di conservazione va valutato come eccezionale e può aver luogo solo in relazione:

- ad esigenze tecniche o di sicurezza del tutto particolari;
- all'indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria;
- all'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria.

CONCLUSIONI

Per tutte le motivazioni tecniche e le previsioni legislative esposte, è' obbligatorio attenersi alle disposizioni contenute nel presente Regolamento, visualizzabile sulla intranet nella sezione Documentazione Privacy.

Nel caso in cui si ravvisino degli “Incidenti informatici” che possano dare luogo a violazione dei dati personali, i Responsabili sono tenuti a trasmettere l’allegato, Scheda di segnalazione al Responsabile del SIA e alla Responsabile protezione dati / DPO Aziendale.

Sistema Socio Sanitario
Regione Lombardia
ASST Nord Milano

REGOLAMENTO INFORMATICO

dell'Azienda Socio Sanitaria Territoriale Nord Milano

ALLEGATO 1

GLOSSARIO INFORMATICO

MALWARE: è un software creato con il solo scopo di causare danni più o meno gravi ad un computer o un sistema informatico su cui viene eseguito, si citano, a mero titolo esemplificativo, alcuni tipi di malware:

- Virus: sono parti di codice che si diffondono copiandosi all'interno di altri programmi, o in una particolare sezione del disco fisso, in modo da essere eseguiti ogni volta che il file infetto viene aperto.
- Worm: questi malware non hanno bisogno di infettare altri file per diffondersi, perché modificano il sistema operativo della macchina ospite in modo da essere eseguiti automaticamente e tentare di replicarsi sfruttando per lo più Internet.
- Trojan horse: software che oltre ad avere delle funzionalità "lecite", utili per indurre l'utente ad utilizzarli, contengono istruzioni dannose che vengono eseguite all'insaputa dell'utilizzatore. Non possiedono funzioni di auto-replicazione, quindi per diffondersi devono essere consapevolmente inviati alla vittima. Il nome deriva dal famoso cavallo di Troia.
- Backdoor: letteralmente "porta sul retro". Sono dei programmi che consentono un accesso non autorizzato al sistema su cui sono in esecuzione.
- Spyware: software che vengono usati per raccogliere informazioni dal sistema su cui sono installati e per trasmetterle ad un destinatario interessato. Le informazioni carpite possono andare dalle abitudini di navigazione fino alle password e alle chiavi crittografiche di un utente.
- Dialer: questi programmi si occupano di gestire la connessione ad Internet tramite la normale linea telefonica. Sono malware quando vengono utilizzati in modo illecito, modificando il numero telefonico chiamato dalla connessione predefinita con uno a tariffazione speciale, allo scopo di trarne illecito profitto all'insaputa dell'utente.
- Hijacker: questi programmi si appropriano di applicazioni di navigazione in rete (soprattutto browser) e causano l'apertura automatica di pagine Web indesiderate.

- Rootkit: i rootkit solitamente sono composti da un driver e, a volte, da copie modificate di programmi normalmente presenti nel sistema. I rootkit non sono dannosi in sé, ma hanno la funzione di nascondere, sia all'utente che a programmi antivirus, la presenza di particolari file o impostazioni del sistema. Vengono quindi utilizzati per mascherare spyware e trojan.
- Scareware: sono così chiamati quei programmi che ingannano l'utente facendogli credere di avere il proprio PC infetto, allo scopo di fargli installare dei particolari malware, chiamati in gergo rogue antivirus, caratterizzati dal fatto di spacciarsi per degli antivirus veri e propri, talvolta anche a pagamento.
- Rabbit: sono programmi che esauriscono le risorse del computer creando copie di sé stessi (in memoria o su disco) a grande velocità.
- Adware:sono programmi software che presentano all'utente messaggi pubblicitari, a fronte di un prezzo ridotto o nullo. Possono causare danni quali rallentamenti del PC e rischi per la privacy in quanto comunicano le abitudini di navigazione ad un server remoto.
- Keylogger: sono programmi in grado di registrare tutto ciò che un utente digita su una tastiera o che copia e incolla rendendo così possibile il furto di password o di dati che potrebbero interessare qualcun altro.
- Rogue antispyware: è un tipo di malware che si finge un programma per la sicurezza del PC, spingendo gli utenti ad acquistare una licenza del programma.
- Bomba logica: è un tipo di malware che "esplode" ovvero fa sentire i suoi effetti maligni al verificarsi di determinate condizioni o stati del PC fissati dall'hacker stesso.

PHISHING: è un tipo di truffa via internet attraverso la quale un aggressore cerca di ingannare la vittima convincendola a fornire informazioni personali sensibili. Si tratta di una attività illegale che sfrutta una tecnica di ingegneria sociale: attraverso l'invio casuale di messaggi di posta elettronica che imitano la grafica, ad esempio, di siti bancari o postali, un malintenzionato cerca di ottenere dalle vittime la password di accesso al conto corrente, le password che autorizzano i pagamenti oppure il numero della carta di credito. L'utente malintenzionato (phisher) spedisce al malcapitato e ignaro utente un messaggio e-mail che simula, nella grafica e nel contenuto, quello di una istituzione nota al destinatario (per esempio la sua banca, il suo provider web, un sito di aste online a cui è iscritto). L'e-mail contiene quasi sempre avvisi di particolari situazioni o problemi verificatesi con il proprio conto corrente/account (ad esempio un addebito enorme, la scadenza dell'account, ecc.) oppure un'offerta di denaro. L'e-mail invita il destinatario a collegarsi ad un link, presente nel messaggio, per evitare l'addebito e/o per regolarizzare la sua posizione con l'ente o la società di cui il messaggio simula la grafica e l'impostazione (Fake login). Il link fornito, tuttavia, non porta in realtà al sito web ufficiale, ma a una copia fittizia apparentemente simile al sito ufficiale, situata su un server controllato dal phisher, allo scopo di richiedere e ottenere dal destinatario dati personali particolari, normalmente con la scusa di una conferma o la necessità di effettuare una autenticazione al sistema; queste informazioni vengono memorizzate dal server gestito dal phisher e quindi finiscono nelle mani del malintenzionato. Il phisher utilizza questi dati per acquistare beni, trasferire somme di denaro o anche solo come "ponte" per ulteriori attacchi.

Sistema Socio Sanitario
Regione Lombardia
ASST Nord Milano

MODELLO DI SEGNALAZIONE "INCIDENT REPORT" PER RESPONSABILI PRIVACY DI UNITA'

…… **li**……

Alla DPO
Dr.ssa Maria Francesca Fasano

Al Direttore SIA
Ing. Pietro Lanzoni

LORO SEDI

Si segnala che in data……presso questa Unità Operativa si è verificato il seguente "Incidente" che potrebbe aver causato delle problematiche relative alla riservatezza dei dati personali.

DESCRIZIONE dell'accaduto

……
……
……
……
……
……
……
……
……
……
……
……
……
……
……

Segnalazione ricevuta da:

_____

Eventuale Utenza Coinvolta(interna/esterna):_____
__

_____
_____

IL RESPONSABILE PRIVACY DI UNITA'

……

SPAM: COME DIFENDERSI

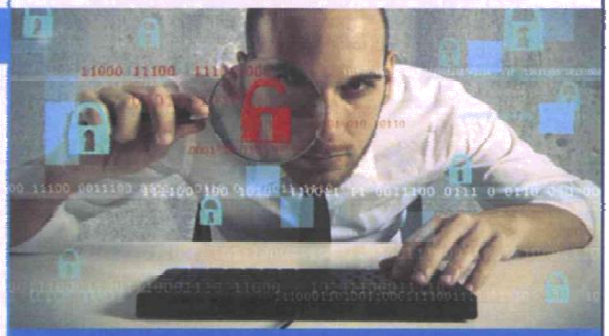
Spamming* o *spam è l'invio, talora massiccio e ripetuto, tramite operatore o con modalità automatizzate, di **comunicazioni non richieste** (via telefono, *e-mail*, fax, sms o mms), senza che il destinatario abbia ricevuto un'**informativa** sul trattamento dei dati personali o abbia prestato il **consenso** a ricevere messaggi. Negli ultimi tempi, lo *spamming* sta interessando anche il mondo dei *social network* e quello dei sistemi di messaggistica per *smartphone* e *tablet*.

Lo ***spammer*** - cioè colui che invia lo *spam* - utilizza riferimenti (*e-mail*, numeri telefonici, ecc.) per l'invio di messaggi promozionali spesso raccolti in modo non lecito o in maniera automatica via Internet (su gruppi *Usenet*, *newsgroups*, *forum*, ecc.), mediante speciali programmi (*spambot*, ecc.) o, più semplicemente, facendo invii massivi a caso ad indirizzi *e-mail* basati sull'uso di nomi comuni

Scopo dello *spamming* è veicolare messaggi pubblicitari, ma tale pratica è legata anche a veri e propri tentativi di truffa, come il *phishing*. In Italia l'invio di messaggi automatizzati a fini promozionali non desiderati è soggetto a sanzioni amministrative e penali.

Come prevenire lo spam?

- **Non diffondere**, soprattutto *on-line*, il tuo indirizzo e-mail o il numero di telefono fisso o mobile;
- Se per ottenere un dato servizio (iscrizione a *newsletter*, acquisti *on-line*, ecc.) devi firmare un documento o iscriverti ad un sito web, **leggi sempre con attenzione le regole privacy e le condizioni d'uso del servizio**, e soprattutto verifica le modalità e le finalità del trattamento dei tuoi dati personali;
- Prendi in considerazione di **utilizzare più indirizzi *e-mail*** per le tue varie esigenze. Ad esempio, potresti crearne uno ad uso **esclusivamente** "commerciale", da impiegare per fare acquisti *on-line*, accedere a servizi su Internet, iscriverti a *newsletter*, ecc.. In questo modo, il rischio di «contagio spam» non coinvolgerebbe gli indirizzi di posta elettronica che utilizzi invece per le tue esigenze quotidiane più importanti (lavoro, amicizia, ecc.);
- Se hai un sito personale o un blog su cui vuoi pubblicare la tua *e-mail*, proteggila con accorgimenti che rendono la vita più difficile ai programmi (*i cosiddetti spider*) capaci di raccogliere in automatico gli indirizzi di posta elettronica per finalità di *spamming*;
- Se invii una *e-mail* a molti destinatari, **non rendere visibili gli indirizzi dei tuoi contatti** e usa la funzione *"destinatario in copia conoscenza nascosta (ccn)"*. Stessa precauzione se frequenti dei *newsgroups*, dove possono essere attivi dei programmi *spider* ;
- Prova ad usare i **filtri *anti-spam*** offerti, ad esempio, da alcuni programmi di posta elettronica, che possono aiutarti a bloccare tutti i messaggi provenienti da un particolare indirizzo. Tali funzioni possono essere disponibili anche per i *social network* e i servizi di messaggistica per *smartphone* e *tablet*;
- **Mantieni in efficienza il tuo pc**, scaricando periodicamente gli aggiornamenti (che contengono anche difese *anti-spam*) per il sistema operativo e gli applicativi più utilizzati, e installa eventualmente un programma *anti-virus* che offra anche una protezione *anti-spam*;
- **Se utilizzi i social network**:
  1) controlla le impostazioni privacy del tuo *account* eventualmente limitando la visibilità del tuo profilo;
  2) se disponibile, utilizza la funzione *"di blocco"* per i soggetti che inviano messaggi indesiderati;
  3) non dare l'amicizia a soggetti sconosciuti;
  4) evita di rendere pubblici sulla tua pagina personale il tuo indirizzo *e-mail* o il numero di cellulare.



Cosa non devi fare

- **Non rispondere allo *spam***: la risposta può consentire allo *spammer* di stabilire che il tuo indirizzo *e-mail* è valido e attivo. Così può continuare a «spammarti» o rivendere il tuo indirizzo verificato a terzi. Può anche tentare di utilizzare il contatto creato per portare avanti tentativi di truffa.
- **Non cliccare su eventuali link** per la cancellazione dell'invio e tantomeno non fornire i tuoi dati personali senza aver prima fatto delle verifiche. Questi link potrebbero essere collegati a sistemi che consentono truffe telematiche e furti di identità, ma potrebbero anche aprire la strada a *software spia* o a virus informatici. Per la stessa ragione, **non devi mai cliccare su collegamenti ipertestuali** inseriti nel corpo del testo o **aprire ed eseguire eventuali allegati**, soprattutto se contengono estensioni tipo «.exe». Per la stessa ragione, se non sei sicuro del mittente, evita di scaricare le immagini eventualmente contenute nel corpo del messaggio *e-mail*.

Differenze tra spam e invii leciti

- Se il contatto e-mail o telefonico è stato **raccolto** con il **consenso del destinatario** o secondo le **modalità previste dalla legge** (es: nell'ambito di un contratto per la fornitura di un qualche servizio), non si può parlare di *spam*.
- In ogni caso, **se le comunicazioni pubblicitarie o altro tipo richieste** (es: invio di *newsletter*, ecc.) **risultano ad un certo punto indesiderate**, è tuo diritto opporti al trattamento dei tuoi dati inviando una *e-mail* al mittente per chiedere la sospensione dell'invio o utilizzando, se disponibili, le procedure *on-line* per la cancellazione dei tuoi dati dal *database* di chi ti invia le comunicazioni.

Come agire contro lo spam?

Se sei una persona fisica puoi:
- presentare segnalazioni, reclami e ricorsi al Garante per la protezione dei dati personali
- rivolgerti al giudice ordinario per l'eventuale risarcimento del danno

Se sei una persona giuridica:
- puoi rivolgerti al giudice ordinario per il risarcimento del danno
- **non** puoi fare segnalazioni, reclami e ricorsi al Garante, che può però intervenire d'ufficio