PROTOCOLLO ETICO ORGANIZZATIVO N. 4/2018

Oggetto: Linee guida in tema di contrasto alla criminalità informatica e presidi in tema di privacy e sicurezza ICT

1. SCOPO

In conformità a quanto previsto dal Decreto Legislativo 8 giugno 2001 n. 231 e norme correlate (di seguito *"Decreto"*), in tema di responsabilità amministrativa da reato degli enti, e di quanto previsto dalla L. 190/2012 e dal D.lgs. 33/2013 SIN S.p.A. - Sistema Informativo Nazionale per lo sviluppo dell'agricoltura (di seguito *"Società"* o *"SIN"*), ha predisposto il Modello di organizzazione, gestione e controllo integrato con il Piano triennale per la prevenzione della corruzione e per la trasparenza (di seguito *"Modello e Piano"*).

In aderenza all'art. 24-*bis* del D.lgs. 231/01, inerente ai delitti informatici ed il trattamento illecito di dati, e con trasversale riferimento ai contenuti della L. 190/12, SIN si impegna ad applicare e a fare applicare al proprio personale il presente Protocollo che si prefigge l'obiettivo di:

- indicare le regole e le procedure da attuare all'interno dell'ente per assolvere con autonomia agli adempimenti nella gestione dei processi e dei flussi di informazioni concernenti *la sicurezza informatica*, sotto il profilo logico, fisico ed organizzativo;
- disciplinare gli aspetti inerenti l'organizzazione ed il controllo delle attività relative alla gestione dei rischi correlati ai "*social media"*.

La finalità è l'osservanza della vigente normativa contro la commissione di reati informatici garantendo che tutte le procedure che coinvolgono i sistemi informatici, dati ed informazioni, avvengano nel rispetto delle disposizioni di legge e che siano svolte in modo corretto e trasparente in modo che non vi possa essere alcuno spazio per attività o comportamenti che, anche indirettamente, possano potenzialmente sfociare negli illeciti sopracitati.

Pertanto, scopo del presente Protocollo è disciplinare le attività menzionate sotto l'aspetto procedurale, comportamentale e decisionale, al fine di prevedere:

- un completo e rigoroso monitoraggio del processo nel suo complesso;
- misure organizzative volte alla ragionevole prevenzione delle ipotesi di reato previste dal D.lgs. n. 231/01 e norme correlate, ed a scongiurare la c.d. *"colpa organizzativa"* dell'ente, nonché dalla L. 190/12;
- misure atte a scongiurare, nello specifico, l'applicazione delle sanzioni contenute nell'art. 24-*bis* del Decreto sui delitti informatici e trattamento illecito di dati, nell'art. 25-*quinquies* D.lgs. 231/01 sui delitti contro la personalità individuale e nell'art. 25-*novies* sui delitti in materia di violazione del diritto d'autore;
- definire le norme di comportamento per l'utilizzazione dei sistemi informatici/telematici dell'ente, assicurando la salvaguardia, l'organizzazione e il corretto uso delle risorse;

- ridurre al minimo i rischi di distruzione e perdita dei dati, di qualunque genere essi siano, in possesso di SIN conservati principalmente su supporti informatici, e ridurre al minimo i rischi derivanti da introduzioni nei sistemi interni e danneggiamento delle informazioni aziendali.

La Direzione Aziendale promuove l'implementazione ed il mantenimento di un sistema per la gestione della sicurezza delle informazioni del SIAN conforme alla norma ISO 27001, con la collaborazione di tutte le strutture aziendali coinvolte.

Il Protocollo assolve, inoltre, il compito di agevolare il monitoraggio del processo da parte dell'Organismo di Vigilanza e del Responsabile per la prevenzione della corruzione e per la trasparenza, ciascuno per quanto di competenza.

2. AMBITO DI APPLICAZIONE

Il presente Protocollo è indirizzato a tutto il personale interno all'ente, nonché al personale esterno (anche consulenti, ad esempio), che abbia accesso a dati ed informazioni, o luoghi, che possono alterare, manipolare e danneggiare i flussi informativi aziendali.

Inoltre, le prescrizioni contenute nel presente Protocollo trovano applicazione anche nell'ambito delle attività svolte da qualsiasi dipendente e/o collaboratore e/o consulente in uno specifico ambiente tecnologico quale p.c., *web*, *tablet* o *smartphone.*

Il presente Protocollo utilizza dei termini che verranno specificati nei paragrafi seguenti.

3. REATI DA PRESIDIARE

Lo scorretto utilizzo dei sistemi informatici potrebbe comportare il rischio di commissione di alcune delle fattispecie delittuose di reato presupposto inserite nell'art. 24-*bis* del D.lgs. 231/01 *"Delitti informatici e trattamento illecito di dati".* Si tratta dei seguenti potenziali reati:

1. Falsità in documenti informatici (art. 491-*bis* c.p.).
2. Accesso abusivo ad un sistema informatico o telematico (art. 615-*ter* c.p.).
3. Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615-*quater* c.p.).
4. Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-*quinquies* c.p.).
5. Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-*quater* c.p.).
6. Installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche (art. 617-*quinquies* c.p.).

7. Danneggiamento d'informazioni, dati e programmi informatici (art. 635-*bis* c.p.).
8. Danneggiamento d'informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635-*ter* c.p.).
9. Danneggiamento di sistemi informatici o telematici (art. 635-*quater* c.p.).
10. Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635-*quinquies* c.p.).
11. Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640-*quinquies* c.p.).

Inoltre, è qui considerato uno dei reati previsti dall'**art. 25-*quinquies* del D.lgs. 231/01**:

- Pornografia virtuale (art. 600-*quater*.1 c.p.).

Infine, sono ricompresi i reati previsti dall'**art. 25-*novies* del D.lgs. 231/01** e norme correlate *"Delitti in materia di violazione del diritto d'autore"* ed in particolare gli illeciti previsti dalla Legge n. 633 del 1941:

- Protezione del diritto d'autore e di altri diritti connessi al suo esercizio (art. 171, art. 171-*bis*, art. 171-*ter*, art. 171-*septies*, art. 171-*octies*, art. 174-*quinquies*, Legge 22 aprile 1941 n. 633).

L'elenco completo dei reati applicabili è indicato nel *"Modello di organizzazione, gestione e controllo ex D.lgs. 231/01 integrato con il Piano triennale per la prevenzione della corruzione e per la trasparenza"* (S-SIN-SMAQ-V2-1001) e nella matrice di rischio di reato.

4. RESPONSABILITÀ

Nell'ambito delle attività in questione le responsabilità sono ripartite come segue:

- al responsabile della **Funzione Sicurezza, in collaborazione con l'Area Infrastruttura e con il Responsabile Protezione Dati personali di SIN,** sono demandati i compiti dell'applicazione e della proposta di aggiornamento e modifica del presente Protocollo. Deve essere segnalato tempestivamente all'Organismo di Vigilanza dell'ente (organismodivigilanza@sin.it) e al Responsabile per la Prevenzione della Corruzione e per la Trasparenza (rpc@sin.it) ogni evento suscettibile di incidere sull'operatività e sull'efficacia del Protocollo stesso;
- i **responsabili delle direzioni/aree/funzioni** coinvolte nelle attività di cui al presente Protocollo, hanno la responsabilità di osservare e farne osservare il contenuto.

La verifica delle proposte di aggiornamento del presente Protocollo avanzate dai responsabili spetta, secondo competenza, all'OdV ed al RPCT.

L'approvazione finale delle modifiche al presente Protocollo spetta al Consiglio di Amministrazione.

Qualora si verifichino circostanze:

- non espressamente regolamentate dal Protocollo;
- che si prestino a dubbie interpretazioni/applicazioni;
- tali da originare obiettive e gravi difficoltà di applicazione del Protocollo medesimo,

è fatto obbligo a ciascun soggetto coinvolto nell'applicazione del presente Protocollo di rappresentare tempestivamente il verificarsi anche di una sola delle suddette circostanze al proprio responsabile onde valutare gli idonei provvedimenti in relazione alla singola fattispecie.

Ciascuna direzione/area/funzione è responsabile della veridicità, autenticità ed originalità della documentazione e delle informazioni rese nello svolgimento dell'attività di propria competenza.

5. GLOSSARIO

REATO INFORMATICO

Sulla base delle Linee guida in materia, per "REATO INFORMATICO" si intende *qualsiasi comportamento, sanzionato dall'ordinamento penale che si realizza per mezzo delle nuove tecnologie o comunque rivolto contro i beni informatici. Può esser considerato reato informatico tanto la frode commessa attraverso l'utilizzo del computer tanto le operazioni volte a danneggiare il sistema informatico*.

SISTEMI E DATI

La punibilità deve essere prevista anche per l'interferenza sia che riguardi i sistemi sia che riguardi i dati informatici. Le Linee guida, infatti, definiscono "SISTEMA D'INFORMAZIONE" *un'apparecchiatura o un gruppo di apparecchi interconnessi o collegati, in grado di trattare automaticamente i dati informatici secondo un programma e i dati stessi immagazzinati e gestiti nelle apparecchiature.* I "DATI INFORMATICI", invece, sono *qualsiasi rappresentazione di informazioni di qualsiasi forma che possa essere trattata da un sistema d'informazione*.

DEFINIZIONI GENERALI

- *User-id*: codice identificativo dell'utente.
- *Password*: parola chiave.
- *Firewall*: programma per prevenire accessi non autorizzati e salvaguardarsi da eventuali attacchi esterni.
- *Virus*: programma che può danneggiare i dati o le applicazioni contenute in un sistema.
- *Worm*: particolare tipo di virus che si diffonde in reti di computer.
- *E-mail*: posta elettronica.
- *Sistema informatico aziendale*: insieme di personal computer portatili e fissi, tutti collegati in rete con server; applicativi e altri strumenti che permettono comunicazioni elettroniche effettuate tramite la posta elettronica interna ed esterna (e-mail) e l'accesso a Internet.

TECNOLOGIE SOCIALI

Per *"tecnologie sociali"* s'intende una vasta gamma di applicazioni quali, a titolo esemplificativo ma non esaustivo:

- *Social Network:* connessioni effettuate attraverso il proprio profilo personale e/o professionale.
- *Social commerce:* acquisti compiuti online e relativa condivisione di opinioni.
- *Blog/Microblog:* esperienze ed opinioni pubblicate e condivise sulla rete.
- *Social gaming:* connessioni effettuate con amici o sconosciuti con il fine di condividere un gioco online.
- *Wikis:* accesso semplice e veloce alla conoscenza dove è possibile ricercare, creare e modificare articoli.
- *Media and file sharing:* condivisione e commenti a foto, video e audio.
- *Forum:* scambio e condivisione di idee, opinioni ed esperienze in *community* aperte con accesso veloce.

6. GESTIONE OPERATIVA DEL PROCESSO

Si precisa che, per una trattazione più approfondita del tema oggetto del presente Protocollo etico organizzativo, si rimanda alle procedure aziendali vigenti, in particolare quelle del sistema di gestione ISO 27001.

CONTROLLO ACCESSI, PROFILI IDENTIFICATIVI E PASSWORD

L'accesso degli utenti ai sistemi informatici interni è consentito ai lavoratori dipendenti, distaccati e ad utenti esterni preventivamente autorizzati, entrambi ottenuti preferibilmente su opportuna lettera di assegnazione utenza e profilo di accesso, quale supporto al lavoro giornaliero.

Ciascun utente autorizzato deve essere fornito di un codice identificativo (*"User-id"* o *"ID"*) che, utilizzato in abbinamento a una password personale, consenta di accedere al sistema.

Codice e password iniziali sono definite dal responsabile della Funzione Sicurezza; la password deve essere composta da una combinazione di numeri e lettere onde consentire un maggior livello di tutela.

Per ogni ambiente applicativo l'ID è unico, utilizzabile solo da una persona e non riutilizzabile per altri; viene disattivato definitivamente alla comunicazione della cessazione del rapporto di lavoro. Nei casi di dimissioni/cessazione di dipendenti/distaccati, di interruzione dei contratti con collaboratori o di cessazione del ruolo dei soggetti terzi cui è stato concesso l'accesso ai sistemi, le credenziali di accesso sono disabilitate con immediatezza; nel caso di variazioni di ruolo dei soggetti precedentemente elencati, le abilitazioni delle credenziali di accesso concesse cono modificate con immediatezza per adeguarle al nuovo ruolo.

Dopo la prima creazione, le password sono a gestione esclusiva dell'utente, che è obbligato a modificarle periodicamente.

A parte l'utente stesso, nessun altro può conoscere la password degli utenti dei sistemi informatici, nemmeno il responsabile della Funzione Sicurezza. Quest'ultimo, dotato di più alta autorità *"informatica"* rispetto agli utenti, ha comunque sempre la possibilità di forzare il sistema; così, in caso di dimenticanza della password da parte di un utente, il responsabile sopra citato crea una nuova password *"temporanea"* che comunica all'utente; quest'ultimo provvede subito a modificarla, divenendo, da quel momento, l'unico conoscitore e gestore della nuova password. Inoltre:

- la password che l'utente è in grado di auto generare è strettamente personale, deve restare segreta e non deve essere comunicata né ai colleghi né a terzi. A questo scopo è obbligatorio non lasciare incustodita, tantomeno visibile o disponibile, la password personale di accesso al personal computer e agli applicativi che la prevedono. A titolo esemplificativo, costituisce violazione del presente Protocollo anche lasciare un post-it contenente la propria password in un luogo facilmente accessibile (ad es. sul monitor, sotto la tastiera del PC, sulla scrivania, ecc.);
- le password permettono l'accesso ai servizi attivati solo ai soggetti espressamente autorizzati; è pertanto indispensabile conservare le password con la massima diligenza per impedire che soggetti terzi ne vengano a conoscenza e segnalare sollecitamente al responsabile della Funzione Sicurezza lo smarrimento, la sottrazione o la dimenticanza delle stesse;
- ogni password deve essere almeno di otto caratteri (preferibilmente alfanumerici), che non formano una parola e che non siano semplici da indovinare (es. nomi di parenti, soprannomi, ecc.);
- le password di accesso ai sistemi informativi hanno una durata massima definita; raggiunto tale termine esse scadono devono essere rinnovate dagli utenti.

Gli utenti hanno la responsabilità di usare i sistemi in modo professionale, etico e conforme alle leggi vigenti, ai regolamenti aziendali nonché al presente Protocollo etico organizzativo. Si precisa che è vietato:

1. l'uso dei sistemi senza preventiva autorizzazione;
2. l'accesso effettuato usando User-id e password diverse da quelle personali;
3. l'uso improprio e dannoso dei social media da parte di un dipendente/collaboratore;
4. ogni altro metodo utilizzato per accedere o utilizzare i sistemi di SIN difformemente dalle Linee guida desumibili dal presente Protocollo e da quanto previsto dalle procedure/policy/istruzioni/regolamenti aziendali.

È altresì proibito copiare e/o utilizzare software in violazione della legge sui diritti d'autore, delle licenze e delle altre tutele giuridiche applicabili.

Si rammenta che effettuare senza permesso e ripetutamente accessi a siti web durante l'orario di lavoro e non per attività lavorativa è considerato assenteismo virtuale in quanto l'ente ha adottato le garanzie che le normative prevedono per il trattamento dei dati sensibili ed i dipendenti/collaboratori, vengono informati, in dettaglio, circa le modalità di utilizzo di internet e delle e-mail e sul fatto che vi siano possibilità che vengano effettuati controlli.

CONTROLLI

SIN ha la facoltà di:

- far procedere alla rimozione immediata di ogni file/applicazione che sarà ritenuto pericoloso per la sicurezza del sistema aziendale ovvero acquisito od installato in violazione delle presenti regole o di quelle applicabili in base alle linee guida desumibili dal presente Protocollo;
- effettuare a campione ispezioni periodiche sulle postazioni di lavoro, anche senza preavviso all'utente per fini di tutela, sicurezza e continuità aziendale ma sempre nel pieno rispetto della normativa applicabile in tal senso;
- utilizzare strumenti quali gli sniffer impostati come spyware oppure utilizzare tecniche di sorveglianza desktop.

VIRUS

Il *virus* è un evento di disturbo/paralisi di un computer che può:

- generare messaggi di disturbo sullo schermo;
- ridurre la quantità di memoria e/o lo spazio disco;
- modificare i dati;
- sovrascrivere o cancellare file;
- rallentare le prestazioni del computer;
- creare problemi nel salvataggio dei dati;
- eliminare tutti i dati presenti sul disco fisso;
- inviare i dati a destinatari estranei o non appropriati;
- dare accesso a soggetti non autorizzati.

Le vie principali di trasmissione dei virus sono:

- pennette usb, cd, dvd (qualora presente il relativo supporto);
- internet e le reti in generale;
- la posta elettronica (è il principale mezzo di diffusione dei virus motivo per il quale occorre prestare attenzione qualora si ricevano e-mail sospette o da destinatari non abituali).

La propagazione di attacchi informatici accompagnati da richieste estorsive nei confronti di numerosi ed eterogenei soggetti economici, e per importi considerevoli, testimonia l'inanità dell'approccio

incentrato nel solo rafforzamento delle barriere *antivirus* e dei sistemi di *recovery*. Contributi della letteratura recente segnalano che la normativa vigente richiede un impegno organizzativo adeguato ed efficiente, idoneo anche ad escludere che nel corso della vicenda info-estorsiva, e per la soluzione di essa, possano essere commessi illeciti da esponenti aziendali nell'interesse/vantaggio dell'ente collettivo aggredito, configurandosi in tal modo la pericolosa e paradossale situazione di commettere un reato presupposto 231 nel momento del pagamento agli estorsori.

Senza contare che i comportamenti devono conformarsi, altresì, alle prescrizioni del Regolamento *Privacy* U.E. 2016/679 che impongono cautele anche rispetto al trattamento dei dati personali accidentalmente, o per fatto illecito del terzo, in violazione dei diritti dei soggetti titolari.

Si rammenta che il *"Ransomware"* (pizzo elettronico) è un tipo di malware che, con la trasmissione di un'e-mail (di un sms o chat) e l'apertura di essa (di un allegato, o cliccando su un link o banner), infetta il sistema informatico e i dati da esso custoditi recapitando la richiesta di riscatto (ransom) per rimuovere la limitazione.

Di prassi, il pagamento è richiesto in Bitcoin, moneta non tracciabile o con voucher anonimo e prepagato MoneyPak, come da dettagliate istruzioni fornite.

La *"sgradita comunicazione"* dei criminali informatici produce contemporaneamente alcuni effetti e prelude spesso a conseguenze rilevanti. L'effetto immediato, infatti, risulta l'infezione digitale del Sistema operativo (i.e.: file personali, documenti, desktop, siti, foto, video, musica, disco rigido e condivisioni di rete). La cifratura e la criptazione integrale rendono i dati immediatamente – ma temporaneamente – illeggibili, non consultabili, non utilizzabili, né recuperabili.

Contestualmente viene richiesto un riscatto da pagare entro un termine perentorio, pena la lievitazione della somma richiesta in prima istanza, dopodiché seguirà automaticamente la distruzione irreversibile dei dati *"congelati"*.

IL PERSONAL COMPUTER

Il personal computer (fisso o mobile) ed i relativi programmi e/o applicazioni affidati al personale sono strumenti di lavoro, pertanto:

- possono essere utilizzati solo per fini lavorativi e non anche per scopi personali;
- vanno utilizzati in modo appropriato;
- devono essere prontamente segnalati all'ente (alla figura incaricata a ricevere segnalazioni) il furto, il danneggiamento o lo smarrimento di tali strumenti.

Per garantire un uso corretto degli strumenti aziendali:

- non è consentito utilizzare strumenti software e/o hardware con modalità diverse da quelle indicate nelle procedure vigenti. Ciò anche perché tali strumenti sono potenzialmente atti ad

alterare, cancellare, modificare, intercettare, falsificare il contenuto di comunicazioni e/o informazioni;

- in particolare, non è consentita l'installazione autonoma, nemmeno sul pc in dotazione, di mezzi di proprietà dell'assegnatario (es. modem, stampanti, altre periferiche, software) onde evitare il pericolo dell'introduzione di virus informatici, nonché alterare la stabilità delle applicazioni del computer;
- non è consentito installare programmi (software) senza specifica autorizzazione scritta e specifico intervento del responsabile della Funzione Sicurezza;
- non è permesso modificare o alterare le configurazioni del pc;
- al termine delle operazioni o in caso di sospensione temporanea delle operazioni stesse (es. allontanamento dal posto di lavoro durante la pausa pranzo) la visibilità dei dati sul monitor deve essere inibita tramite un'adeguata procedura [premere contemporaneamente i tasti "*Alt", "Ctrl" e "Canc"* e cliccare su *"blocca computer"* (successivo uso della password per la ripartenza), oppure spegnere il computer, oppure usare lo *"screen saver"* temporizzato e successiva riattivazione tramite la password]. Ciò qualora non sia stato già implementato un automatico spegnimento temporaneo del pc trascorso un predeterminato periodo di tempo senza che sia stato utilizzato;
- se l'utente si accorge di avere accesso a dati o programmi di trattamento di dati personali non di sua competenza, è tenuto ad informare subito il Responsabile della protezione dei dati personali in ottemperanza alla normativa privacy;
- i computer vanno sempre protetti da condizioni climatiche sfavorevoli quali elevata temperatura e umidità, vapori, liquidi, fumi, polvere od altre sostanze contaminanti;
- al termine dell'uso del computer occorre sempre chiudere i programmi secondo le appropriate procedure di sicurezza. È vietato premere direttamente il tasto di spegnimento del pc senza eseguire la procedura sopradescritta, soprattutto se non sono state chiuse tutte le applicazioni;
- è tassativamente vietata la detenzione di materiale non in regola con la normativa sul diritto di autore (SIAE) e pedo-pornografico, anche virtuale, in quanto costituente reato.

UTILIZZO DELLA RETE AZIENDALE

Le unità di rete (server, cui sono applicate specifiche protezioni per l'accesso ai locali ove sono custoditi) sono aree di condivisione di informazioni strettamente aziendali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto, qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in tali unità. Colui che dovesse creare in rete le cosiddette *"cartelle condivise"* deve aver cura di concederne l'accesso, tramite l'apposita procedura prevista dal sistema operativo adottato, solo a chi debba esserne coinvolto per motivi di servizio.

Per facilitarne la gestione, la denominazione della cartella condivisa deve sempre essere intestata con le generalità dell'autore.

Il Datore di lavoro può limitare l'utilizzo della rete aziendale per fini non attinenti all'attività lavorativa limitando i tempi di accesso o inibendo la possibilità di accedere ai social network.

POSTA ELETTRONICA

La posta elettronica (e-mail) è da considerare uno strumento di lavoro.
Le seguenti regole costituiscono requisiti per rendere lecito e corretto il ricorso alla posta elettronica:

- l'uso della e-mail deve sempre essere rispettoso delle norme di legge (es.: segreto commerciale, diritto d'autore, riservatezza, privacy ecc.);
- non è consentito inviare o memorizzare messaggi (interni ed esterni) di natura oltraggiosa e/o discriminatoria in relazione a genere, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica anche in ottemperanza ai contenuti dell'art. 25-*terdecies* D.lgs. 231/01 *"Razzismo e xenofobia"*;
- la posta elettronica diretta all'esterno della rete informatica aziendale può essere potenzialmente intercettata da estranei e, dunque, non deve essere preferibilmente utilizzata per inviare documenti di lavoro aventi natura estremamente riservata;
- per ogni comunicazione, interna ed esterna che abbia contenuti rilevanti/riservati, è preferibile adottare le ordinarie procedure di corrispondenza;
- l'uso personale della posta elettronica è consentito a patto che esso non interferisca con l'attività lavorativa, non si configuri come un irragionevole dispendio di risorse e non pregiudichi le attività aziendali;
- non è consentito l'utilizzo dell'indirizzo di posta elettronica aziendale per la partecipazione a dibattiti o forum, salvo diversa ed esplicita autorizzazione scritta del proprio Responsabile;
- in ogni caso, l'utilizzo dei servizi e-mail deve essere limitato e compatibile con l'orario di lavoro e le regole stabilite dall'ente.

È consigliato impostare un messaggio di risposta e-mail automatica che, in caso di assenza dal lavoro di un utente, informi il mittente di eventuali comunicazioni:

- della durata dell'assenza;
- dei riferimenti telefonici o e-mail del collega-sostituto da contattare.

Occorre prestare attenzione ai messaggi di posta elettronica che provengono da persone o enti sconosciuti. Si deve fare attenzione soprattutto ai virus nascosti nei file eseguibili o ai macro-virus presenti nei documenti; in tali casi, non bisogna aprire gli allegati in quanto potrebbero contenere virus (l'estensione degli allegati *"infetti"* è spesso .PST, LPS, .EXE oppure contiene in oggetto nomi di persone o frasi ad effetto che suscitano normalmente curiosità). Pertanto, non si deve aprire nessun tipo

di allegato qualora proveniente da un mittente sconosciuto oppure, anche se il mittente è conosciuto, l'oggetto della mail o il suo contenuto appare sospetto o inusuale (piuttosto occorre informare immediatamente il responsabile della Funzione Sicurezza e attenersi alle conseguenti istruzioni da questi impartite), né si devono inviare e-mail sospette ad altri utenti sia interni che esterni.

Il Datore di lavoro può, così come raccomandato dal garante della Privacy:

- realizzare anche indirizzi condivisi tra più lavoratori;
- attribuire al lavoratore un ulteriore indirizzo di posta, oltre a quello di lavoro già fornito dall'ente, destinato ad uso esclusivamente personale;
- stilare una *"black list"* di siti web negativi. anche ai fini della protezione della sicurezza dei sistemi dagli attacchi esterni, bloccandone preliminarmente l'accesso;
- adottare misure come la configurazione di filtri che prevengono l'accesso ai suddetti portali web.

INTERNET

SIN ammette l'uso di Internet da parte dei propri dipendenti unicamente per acquisire o scambiare informazioni finalizzate alla realizzazione degli obiettivi, della missione e delle politiche dell'ente.

L'installazione di modem o di altri strumenti di interconnessione deve essere autorizzata dal responsabile competente, su richiesta scritta del diretto superiore dell'utente.

Per quanto riguarda la navigazione in Internet, valgono le seguenti norme comportamentali:

- in linea generale, l'uso personale di internet non è consentito (nel caso in cui si intenda consentire l'utilizzo personale o lo si intenda limitare, modificare); occorre evitare di navigare in siti non attinenti allo svolgimento delle mansioni assegnate, soprattutto in quelli che possono rivelare le opinioni politiche, sindacali, religiose o di genere del dipendente o del collaboratore in quanto il sistema effettua automaticamente la registrazione degli accessi e, quindi, è potenzialmente idoneo a rivelare dati sensibili concernenti tali soggetti;
- è vietata ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa;
- non è permessa la partecipazione, per motivi non professionali, a forum, l'utilizzo di chat line, di bacheche elettroniche e le registrazioni in guest book anche utilizzando pseudonimi (o nicknames);
- non è consentita l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di *remote banking*, acquisti *on-line* e simili, salvo casi direttamente autorizzati per iscritto dal responsabile della Funzione Sicurezza (sentito preventivamente il Consiglio di Amministrazione);
- non è consentito scaricare software, soprattutto se gratuiti (*freeware* e *shareware),* prelevato da siti Internet.

Con riferimento all'utilizzo di collegamenti wireless (WIFI), devono essere adottate specifiche misure precauzionali ed essere impartite istruzioni per una navigazione in Internet che rispetti la normativa vigente, le procedure interne di SIN ed i principi etici fondanti dell'ente.

ATTIVITÀ DI ROUTINE PER UN CORRETTO UTILIZZO DELLE APPARECCHIATURE IN DOTAZIONE

In base ai principi sopra evidenziati, tutti gli utenti che utilizzano strumenti appartenenti ai sistemi informatici aziendali:

- hanno la responsabilità di mantenere le risorse in buono stato di conservazione;
- non devono eseguire alcuna attività che sprechi o monopolizzi le risorse e il buon uso dei sistemi aziendali;
- non devono mai aprire o cercare di riparare personalmente le apparecchiature in dotazione;
- devono attuare le procedure minimali di gestione/manutenzione dei personal computer a disposizione.

SIN effettua un accertamento sistematico dell'operatività ed efficacia delle procedure di back-up ed archiviazione dei dati. Quotidianamente i destinatari del presente Protocollo devono:

- salvare, a intervalli regolari, i dati inseriti. Durante una sessione prolungata di lavoro, salvare ripetutamente il proprio lavoro, riducendo l'intervallo di salvataggio in caso di riscontrata instabilità del sistema. Infatti, nel caso di crash o blocco del computer/programma, il lavoro non salvato andrebbe perso;
- per evitare di perdere informazioni in caso di problemi sul pc, assicurarsi che avvenga il salvataggio sul server di rete di tutti i documenti importanti per lo svolgimento della propria mansione o dell'attività aziendale, conformemente alle istruzioni ricevute;
- conservare i supporti fisici che contengono eventuali copie di back up in un luogo sicuro, possibilmente chiuso a chiave; non portarli al di fuori dei luoghi aziendali;
- le copie effettuate su supporto mobile (ad es. pennette USB), qualora autorizzate, devono essere custodite sotto la diretta responsabilità dell'utente e devono essere opportunamente crittografate;
- in caso di cessato utilizzo dei supporti di memorizzazione elettronica o comunque automatizzata, occorre rendere tecnicamente irrecuperabili i dati registrati (anche in caso di immediato riutilizzo del supporto per la registrazione di nuovi dati), oppure distruggere i supporti stessi. Procedere ad una normale cancellazione di file non significa rendere tecnicamente irrecuperabili i dati registrati: occorrerà procedere con la formattazione.

Periodicamente è opportuno eseguire la procedura di scandisk attraverso cui si verifica la presenza di eventuali errori nei file e nelle cartelle del disco rigido e si controlla la superficie fisica del disco, la procedura di deframmentazione del disco che serve ad aumentare le prestazioni del computer.

Occorre evitare di sovraccaricare il proprio elaboratore correndo il rischio di un blocco (con conseguente perdita di dati) aprendo, ad esempio, contemporaneamente più sessioni di lavoro. Inoltre, non si devono eseguire comandi o procedure di sistema di cui non si conosca esattamente l'effetto.

Quando si crea o si salva un file (soprattutto con la procedura *"salva con nome"*) è indispensabile verificare preventivamente che sia stato effettuato il salvataggio dei dati, e che non esista nessun altro file col nome prescelto all'interno della directory: il contenuto del file preesistente potrebbe andare perso.

Nonostante la presenza del software antivirus, è possibile che si possano inavvertitamente installare nei computer virus informatici non identificati o riconoscibili; pertanto, nel caso si evidenzino anomalie di funzionamento del computer, occorre darne immediata segnalazione al responsabile della Funzione Sicurezza.

7. PRIVACY E SICUREZZA ICT

La struttura aziendale responsabile della privacy e sicurezza, a tutela di SIN in qualità di Titolare e Responsabile del trattamento dei dati, e del Direttore Generale avente delega in materia, provvede – in collaborazione con il Responsabile protezione dati di SIN - al periodico riesame su base annuale o a fronte di cambiamenti o organizzativi, ed all'aggiornamento del modello organizzativo della Privacy e della documentazione richiesta ai sensi della normativa vigente, in particolare il Regolamento (UE) 2016/679 e dei suoi decreti attuativi, ed opera in maniera proattiva affinché siano attuate le azioni in esso previste dalle diverse strutture competenti.

La struttura aziendale responsabile della privacy e sicurezza provvede, altresì, in collaborazione con il Responsabile protezioni dati, a definire la periodicità con cui deve essere eseguita la formazione in materia privacy e sicurezza delle informazioni ed a pianificarla in accordo a tale periodicità d'intesa con l'ufficio del personale.

I fornitori/consulenti/collaboratori devono sottoscrivere appositi impegni nel caso trattino dati personali di cui SIN e/o i Committenti siano Titolari.

Nei contratti/ordini che SIN stipula con fornitori, consulenti, e collaboratori vengono inseriti i requisiti per la gestione della sicurezza delle informazioni definiti da SIN, qualora indicato dal RUP nella determina a contrarre.

8. SISTEMA DISCIPLINARE

Il presente Protocollo etico organizzativo costituisce parte integrante del Modello organizzativo 231 e Piano prevenzione corruzione e trasparenza della Società. L'inosservanza dei principi e delle regole ivi

contenuti rappresenta pertanto una violazione di detto Modello e Piano e comporta l'applicazione delle specifiche misure disciplinari di cui al Codice Disciplinare e Regolamento Sanzionatorio (S-SIN-SPER-I7-14001).

9. RICHIAMO ALLE PROCEDURE INTERNE COLLEGATE

Si veda l'Elenco generale Documenti di Sistema (S-SIN-SMAQ-L2-11001).

10. RIFERIMENTI NORMATIVI ESSENZIALI

Decreto Legislativo 8 giugno 2001 n. 231 e s.m.i.
Legge 6 novembre 2012 n. 190 e s.m.i.
Per completezza informativa, si rimanda ai riferimenti normativi elencati nel *"Modello di organizzazione, gestione e controllo ex D.lgs. 231/01 integrato con il Piano triennale per la prevenzione della corruzione e per la trasparenza"* (S-SIN-SMAQ-V2-1001).