REGOLAMENTO PER LA SICUREZZA DEL TRATTAMENTO DEI DATI

EMISSIONE DEL DOCUMENTO

Azione	Data	Nominativo	Funzione
Delibera n. 15	20/05/2022	Consiglio di Amministrazione	

REGISTRO REVISIONI

Rev.	Data	Autore	Descrizione

Sommario

1. Premessa

La sicurezza delle informazioni costituisce un valore imprescindibile per l'Organizzazione e per i suoi lavoratori, in particolare nell'ambito della postazione di lavoro e dei sistemi informatici.

Premesso che l'utilizzo delle risorse informatiche e telematiche deve sempre ispirarsi al principio della diligenza e correttezza, l'Organizzazione ha adottato il presente "***Regolamento per la sicurezza del trattamento dei dati***" (d'ora in avanti "Regolamento"), volto ad evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla sicurezza nel trattamento dei dati (personali e non), dei documenti e delle apparecchiature elettronico informatiche e volto ad adottare idonee misure di sicurezza per assicurare la disponibilità e l'integrità di sistemi informativi.

Lo scopo del presente Regolamento è quello di indicare i limiti entro cui i fruitori possono legittimamente usare gli strumenti elettronici messi a disposizione dall'Organizzazione al fine di uno svolgimento proficuo e più agevole della propria attività (personal computer, smartphone, tablet, etc.), evitando di esporre sé stessi e/o la propria Organizzazione a gravi conseguenze che, in taluni casi, determinano ingenti sanzioni pecuniarie e, nei casi più gravi, possono investire il diritto penale.

Il Regolamento è stato implementato per tutelare la sicurezza dei sistemi informativi dell'Organizzazione, assicurando la disponibilità delle risorse informative e dei dati, l'integrità dei sistemi e dei dati e la riservatezza delle informazioni.

Il Regolamento, inoltre, oltre a dettare una disciplina per l'utilizzo degli strumenti aziendali, è da considerarsi uno **strumento di formazione e sensibilizzazione** per il personale nell'ambito degli obiettivi e delle Politiche di sicurezza delle informazioni adottate dall'Organizzazione.

L'Organizzazione ha ritenuto inoltre di porre in essere adeguati e commisurati sistemi di controllo sul corretto utilizzo degli strumenti e delle risorse informatiche e telematiche, senza che ciò possa in alcun modo invadere e violare la sfera personale del lavoratore e quindi il suo diritto alla riservatezza ed alla dignità.

A tal fine il presente strumento regolamenta l'utilizzo degli strumenti elettronici atti a rendere la prestazione lavorativa in conformità alle prescrizioni dell'art. 4, comma 2, Legge 300/1970 (come modificato dall'art. 23 del D.Lgs. 151/2015), della Deliberazione n. 13 del 01/03/2007 del Garante per la protezione dei dati personali "Linee guida per la posta elettronica ed internet", del General Data Protection Regulation - GDPR (Regolamento 679/2016/UE) e tutte le sue norme attuative vigenti.

Le prescrizioni di seguito previste si aggiungono ed integrano le specifiche istruzioni eventualmente già fornite agli incaricati ed agli specifici responsabili designati. Esse inoltre integrano le eventuali informazioni già fornite agli interessati in ordine alle ragioni e alle modalità dei possibili controlli o alle conseguenze di tipo disciplinare in caso di violazione delle stesse.

2. Oggetto e campo di applicazione del Regolamento

L'oggetto del Regolamento è:

- disciplinare le modalità di utilizzo di qualsiasi dotazione per il trattamento dei dati messa a disposizione dall'Organizzazione, sia all'interno sia all'esterno delle sedi di lavoro, ivi compresi eventuali siti di telelavoro, atta a rendere la prestazione lavorativa;
- elencare i doveri che ciascun utilizzatore è tenuto ad osservare.

L'utilizzo delle risorse e dei servizi è subordinato al rispetto da parte degli utilizzatori del presente Regolamento, oltre che delle norme civili, penali e amministrative applicabili.

Il Regolamento si applica a tutti i dipendenti, senza distinzione di ruolo e/o livello, a tutti i collaboratori dell'Organizzazione a prescindere dal rapporto contrattuale con la stessa intrattenuto e a chiunque abbia in dotazione, anche temporaneamente, risorse informatiche e telematiche di proprietà dell'Organizzazione o ad essa affidate. Tali soggetti, nell'ambito del presente Regolamento, sono indicati nel seguito anche come "Utente", "Utilizzatore" o "Incaricato".

Il presente Regolamento si applica a qualsiasi dotazione ICT intesa come risorsa informatica e/o telematica (a titolo esemplificativo e non esaustivo computer, notebook, server, software, rete, utenza, file, cartella di rete, internet key, telefono, tablet, smartphone, modem, ecc..), di seguito indicata anche come strumento elettronico, messa a disposizione dall'Organizzazione all'Utente per rendere la prestazione lavorativa.

3. Generale

Tutti gli strumenti elettronici affidati all'Utente sono da considerarsi uno **strumento di lavoro**. Possono essere utilizzati solo per fini professionali (in relazione alle mansioni assegnate) e non a fini personali. Quindi ogni utilizzo non inerente l'attività lavorativa è vietato. La deroga alla presente condizione è consentita solo in caso di specifica approvazione da parte del Titolare o suo delegato.

Tutti gli strumenti elettronici affidati all'Utente non possono essere utilizzati per scopi illeciti e devono essere custoditi con cura ed in modo appropriato evitando ogni possibile forma di danneggiamento.

Gli strumenti elettronici devono essere spenti al termine della propria sessione lavorativa giornaliera, in caso di assenze prolungate dall'ufficio o in caso di loro inutilizzo. Qualora l'elaboratore sia utilizzato da più incaricati, alla conclusione dei lavori è necessario disconnettere il proprio account dal sistema. Prima di effettuare la disconnessione chiudere i programmi rimasti eventualmente aperti. In questo modo la persona che utilizzerà il personal computer in seguito potrà comunque effettuare la procedura di autenticazione. Lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso.

Si fa presente che tutti i dischi o altre unità di memorizzazione locali potrebbero non essere soggetti a salvataggio da parte del sistema informatico dell'Organizzazione. Pertanto gli Utenti sono tenuti a memorizzare la documentazione lavorativa esclusivamente sui server dell'Organizzazione.

È indispensabile che nessun dato personale degli Utenti non inerente l'attività lavorativa sia presente sulle risorse informatiche dell'Organizzazione neppure provvisoriamente.

Per i PC non appartenenti alla rete dell'Organizzazione, non avendo accesso diretto ai server e di conseguenza ai salvataggi periodici, i dati devono essere conservati sul disco locale e periodicamente salvati secondo le istruzioni impartite dall'Amministratore di sistema o dal Responsabile IT.

Ogni Utente è responsabile della propria postazione informatica, della propria casella di posta elettronica e del contenuto dei messaggi da essa inviati. È inoltre responsabile della segretezza delle credenziali di accesso alla rete e ai software al cui utilizzo è stato autorizzato.

Ogni Utente è tenuto ad osservare tutte le misure di protezione e sicurezza atte ad evitare rischi di distruzione o perdita accidentale dei dati, accesso non autorizzato, trattamento non consentito o non conforme alle finalità della raccolta.

Gli Utenti sono tenuti a mantenersi aggiornati, prendendo visione delle eventuali disposizioni emanate e divulgate tramite pubblicazione in area dedicata nella rete informatica dell'Organizzazione, tramite posta elettronica o tramite altro strumento cartaceo (avviso, disposizione, regolamento, ecc.).

Resta inteso che tutte le risorse informative, sia in termini di strumenti che in termini di dati, rimangono di proprietà dell'Organizzazione e che l'Utente è tenuto a restituire la totalità delle risorse utilizzate nel momento in cui dovesse cessare il rapporto con l'Organizzazione o nel caso in cui gli venisse richiesto da quest'ultima.

Gli Utenti sono tenuti a dare tempestiva comunicazione, preferibilmente in forma scritta, di qualsiasi anomalia relativa al sistema informativo aziendale al Titolare o suo delegato affinché la stessa venga valutata dal personale all'uopo incaricato e gestita nel rispetto delle procedure di sicurezza dell'Organizzazione.

4. Regole per gli accessi

L'accesso alla rete informatica dell'Organizzazione e l'utilizzo degli strumenti elettronici dati in affidamento all'Utente è consentito solo attraverso specifiche credenziali di autenticazione, che consistono in un codice per l'identificazione (username) dell'incaricato associato a una parola chiave (password) riservata conosciuta solamente dal medesimo (in alternativa in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato oppure in una caratteristica biometrica dell'incaricato).

Gli accessi ed i permessi degli Utenti garantiscono i profili di autorizzazione degli incaricati in ambito di trattamento dei dati, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.

Ne consegue che gli Utenti possono effettuare esclusivamente i trattamenti di dati personali che rientrano nel proprio ambito lavorativo e per i quali hanno ricevuto specifico incarico. Tali trattamenti devono essere effettuati esclusivamente in conformità alle finalità previste e alle informazioni comunicate agli Interessati.

L'Utente è tenuto a modificare la parola chiave (password) assegnatagli al primo accesso tenendo conto di quanto segue:

- la password deve essere complessa (a titolo esemplificativo: deve contenere lettere e numeri e/o simboli, minimo 8 caratteri, minuscole, Maiuscole);
- la password non deve essere agevolmente riconducibile all'Utente (a titolo esemplificativo non deve essere identica allo username, non deve essere la data di nascita ecc.);
- la sequenza delle password non può essere la medesima di quelle precedenti;
- le credenziali di autenticazione non utilizzate da almeno sei mesi sono automaticamente disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica;
- le credenziali sono disattivate anche in caso di perdita delle qualità che consentono all'Utente, in qualità di incaricato, l'accesso al sistema informatico e ai dati personali in esso custoditi o all'area ad accesso ristretto;
- è vietato affidare al sistema operativo la memorizzazione automatica delle password e l'Utente è tenuto a digitare la password ad ogni accesso;
- è attivo un sistema di blocco delle credenziali di autenticazione in caso di errato inserimento delle stesse per un numero di volte consecutive superiore ad una soglia predefinita, comunicata dal sistema;
- il sistema richiede la modifica della parola chiave (password) ogni sei mesi e, in caso di trattamento di dati sensibili e/o giudiziari, ogni tre mesi;
- sul sistema sono impostati time-out di inattività e screen-saver che, in caso di inattività sullo strumento di durata superiore ad un lasso temporale predefinito, richiedono all'Utente il re-inserimento delle proprie credenziali di autenticazione.

Il codice di identificazione non deve essere comunicato ad alcuno e deve essere custodito dall'Utente con la massima diligenza e non divulgato, seguendo scrupolosamente le indicazioni impartite dall'Organizzazione.

È assolutamente proibito accedere alla rete e ai programmi con un codice di identificazione Utente diverso da quello assegnato.

L'Utente è tenuto ad avvisare prontamente l'ufficio competente al riguardo nell'ipotesi di smarrimento dei dati di accesso.

In caso di prolungata assenza o impedimento di un Utente che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema, il responsabile IT (o l'Amministratore di sistema o l'incaricato alla custodia delle credenziali, se designati), su indicazione della Direzione, al fine di assicurare la disponibilità dei dati e/o degli strumenti elettronici, potrà resettare la componente riservata della credenziale di autenticazione, per consentire l'accesso ad un altro Utente indicato dalla Direzione.

Per le utenze amministrative si utilizzerà la procedura della busta chiusa, che prevede la comunicazione delle proprie credenziali privilegiate di autenticazione solo ed esclusivamente al soggetto incaricato alla custodia delle credenziali, tramite documento sottoscritto dall'Utente, sigillato in busta chiusa e consegnato brevi manu al soggetto su indicato.

L'Utente, terminato il periodo di assenza o impedimento, sarà immediatamente informato in merito all'intervento effettuato e dovrà modificare la propria componente riservata della credenziale di autenticazione.

5. Divieti

È vietato, salvo preventiva ed espressa autorizzazione dell'Organizzazione:

- l'uso di programmi diversi da quelli ufficialmente installati;
- installare, modificare e aggiornare i software autonomamente, se non inclusi nell'elenco software autorizzati;
- modificare le caratteristiche impostate sul proprio personal computer e procedere ad installare dispositivi di memorizzazione, comunicazione o altro;
- utilizzare strumenti software e/o hardware atti ad intercettare, falsificare, alterare o eliminare il contenuto di comunicazioni e/o documenti informatici;
- utilizzare e conservare sul sistema informatico dell'Organizzazione di file non attinenti l'attività lavorativa;
- violare l'integrità di dati personali;

- compromettere l'integrità dei sistemi;
- saturare le risorse in misura tale da compromettere l'efficienza del sistema informativo dell'Organizzazione;
- compiere atti di criminalità informatica;
- consentire l'accesso alla rete e/o condividere la rete con soggetti non autorizzati;
- usare false identità;
- violare la sicurezza, trasferire, comunicare, diffondere, intercettare, accedere a dati per i quali non si ha specifica autorizzazione;
- collegare alla rete aziendale computer personali o computer non assegnati dall'Organizzazione;
- accedere ad aree, chiaramente definite e segnalate dall'Organizzazione, che contengono informazioni sensibili o critiche e strutture di elaborazione delle informazioni, se non specificatamente autorizzati;
- consentire l'accesso alle aree in cui si esegue il trattamento dei dati a personale esterno non autorizzato;
- trasferire all'esterno del sito, anche fisicamente, le apparecchiature, informazioni o software senza preventiva autorizzazione.

Si evidenzia che alcune delle violazioni di cui sopra sono sanzionabili anche penalmente.

6. Politiche di "schermo pulito"

Al fine di ridurre il rischio di accesso non autorizzato ad informazioni aziendali, è necessario che l'Utente segua delle politiche di "schermo pulito". In particolare è fondamentale che presti particolare attenzione alle schermate a video contenenti informazioni non pubbliche. È quindi opportuno che tali schermate siano mantenute solo per il tempo strettamente necessario.

7. Supporti removibili

I supporti rimovibili contenenti dati personali, se non utilizzati, devono essere distrutti o resi inutilizzabili prima di procedere al loro smaltimento. Tali supporti possono essere utilizzati da altri Incaricati se le informazioni precedentemente in essi contenute sono inintelligibili e tecnicamente in alcun modo ricostruibili.

In caso di utilizzo di supporti di origine esterna l'Utente deve procedere all'esecuzione di una scansione anti-malware degli stessi e deve disattivare l'esecuzione automatica dei contenuti.

In ogni caso, i supporti magnetici contenenti dati sensibili devono essere dagli Utenti adeguatamente custoditi in locali o in soluzioni di stoccaggio ad accesso ristretto e controllato (a titolo esemplificativo, armadi o cassetti chiusi a chiave, casseforti e simili).

L'uso di supporti esterni deve essere limitato a quelli necessari per le attività dell'Organizzazione.

È vietato l'utilizzo di supporti rimovibili personali.

L'Utente è responsabile della custodia dei supporti e dei dati aziendali in essi contenuti.

8. Dispositivi portatili

L'Utente è responsabile dei dispositivi portatili assegnatogli dall'Organizzazione e deve custodirli con diligenza, adottando tutti i provvedimenti che le circostanze rendono necessari per evitare danni o sottrazioni.

I dispositivi portatili, proprio per le loro intrinseche caratteristiche, sono più vulnerabili dei dispositivi fissi. Per tale motivo, oltre alle politiche adottate per gli strumenti informatici fissi, occorrono accorgimenti aggiuntivi. Quindi, al fine di minimizzare il rischio associato al furto, all'uso fraudolento e all'accesso di persone non autorizzate alle informazioni presenti sui dispositivi, dovrà essere valutata con il Responsabile IT, in base al tipo di trattamenti eseguiti con tali strumenti, l'opportunità di dotare i dispositivi portatili di un sistema di cifratura dei dati contenuti nell'hard disk, affinché, qualora venga superato il meccanismo di autenticazione dell'accesso, comunque i dati risultino assolutamente indecifrabili.

I dispositivi portatili, al fine di garantire il controllo, l'aggiornamento e l'allineamento alle politiche di sicurezza dell'organizzazione, devono essere periodicamente connessi, direttamente o tramite connessione protetta, alla rete dell'Organizzazione, per la durata necessaria.

9. Utilizzo della rete Internet e dell'account di posta elettronica

La navigazione in Internet ed il sistema di posta elettronica sono mezzi di comunicazione, informazione e trasmissione. L'uso della posta elettronica e della rete Internet, nelle sue numerose funzionalità, è consentito esclusivamente per gli scopi attinenti alle mansioni lavorative assegnate, salvo preventiva ed espressa autorizzazione dell'Organizzazione.

I dati che vengono inviati mediante il sistema di posta elettronica dell'Organizzazione sono di proprietà della stessa.

La casella di posta elettronica assegnata all'Utente è uno strumento di lavoro. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

È fatto divieto di utilizzare le caselle di posta elettronica assegnate e/o messe a disposizione dall' Organizzazione per motivi diversi da quelli strettamente legati all'attività lavorativa e per motivi non attinenti allo svolgimento di mansioni lavorative assegnate.

La "personalizzazione" dell'indirizzo di posta elettronica, ovvero la possibilità che esso contenga riferimenti al nome e cognome dell'utente, non comporta il fatto che la stessa venga considerata "privata", in quanto si tratta comunque di uno strumento di esclusiva proprietà dell'azienda / dell'Ente, messo a disposizione di dipendenti e collaboratori a vario titolo al solo fine dello svolgimento delle proprie mansioni lavorative.

La casella di posta elettronica deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.

Prima di aprire i file allegati ai messaggi di posta elettronica, è necessario identificare il mittente e porre particolare attenzione alla tipologia del file stesso, in caso in cui non si conosca il mittente è consigliabile cancellare tutto, messaggio ed allegato, o sottoporlo a verifica da parte del servizio IT onde evitare attacchi informatici. E' comunque sconsigliato eseguire file allegati ai messaggi di posta elettronica.

Sarà comunque consentito accedere alla casella di posta elettronica dell'Utente per ogni ipotesi in cui si renda necessario per le esigenze dell'Organizzazione, tramite apposita procedura.

Al fine di ribadire agli interlocutori la natura della casella di posta elettronica assegnata dall'Organizzazione, i messaggi devono contenere un avvertimento standardizzato nel quale sia dichiarata la natura non personale dei messaggi stessi.

Inserire nei messaggi di posta elettronica la seguente dicitura:

> *"Questa comunicazione e ogni eventuale file allegato sono ad uso esclusivo del destinatario e potrebbero contenere informazioni riservate. Se non siete l'effettivo destinatario, o un dipendente, o la persona responsabile della consegna della comunicazione, e se l'aveste ricevuta per errore, ci scusiamo per l'accaduto e Vi invitiamo cortesemente a darcene notizia e a distruggerla. Il messaggio ed eventuali file allegati non hanno natura personale e le eventuali risposte alla presente potranno essere conosciute da più soggetti e unità operative all'interno di A.S.P.A. - Azienda Speciale Consortile Servizi alla Persona dell'Asolano, che a vario titolo abbiano interesse ad assolvere le specifiche richieste o esigenze oggetto della comunicazione. Qualsiasi modifica o distribuzione a terzi è assolutamente vietata. Vi ricordiamo, inoltre, che la comunicazione, la diffusione, l'utilizzo e/o la conservazione dei dati ricevuti per errore, costituiscono violazioni alle disposizioni del Regolamento Generale sulla protezione dei dati personali 679/2016 dell'Unione Europea e sono sanzionabili ai sensi dell'art. 616 del Codice Penale."*

In caso di violazione o inadempimento di quanto riportato al presente paragrafo in merito all'utilizzo della posta elettronica, l'Organizzazione procederà ad impedire all'Utente la possibilità di collegamento alla casella di posta elettronica assegnata e si procederà per l'eventuale accertamento di responsabilità disciplinari, in caso di personale dipendente, o contrattuali in caso di professionisti e/o collaboratori.

L'Organizzazione mette a disposizione di ciascun lavoratore, con modalità di agevole esecuzione, apposite funzionalità di sistema che consentano di inviare automaticamente, in caso di assenze programmate, messaggi di risposta che contengano le "coordinate" di altro soggetto o altre utili modalità di contatto.

È assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati allo svolgimento delle mansioni lavorative assegnate, salvo preventiva ed espressa autorizzazione dell'Organizzazione.

È assolutamente proibita la navigazione in Internet qualora il contenuto dei siti sia di natura oltraggiosa e discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.

Il sistema di sicurezza adottato e interposto tra la rete dell'Organizzazione e la rete Internet potrà impedire l'accesso a siti web indesiderati, attraverso la valutazione del contenuto o per l'appartenenza ad una "black list".

Per ridurre il rischio di attacchi informatici durante la navigazione, posizionare il cursore del mouse sul link interessato, osservandone il percorso sulla barra del browser: se è un file eseguibile potrebbe trattarsi di un programma malevolo (ad esempio di un programma che potrebbe collegare l'Utente a un altro indirizzo internet, non sicuro).

Nel caso il software antivirus rilevi la presenza di un virus, l'Utente dovrà immediatamente sospendere ogni elaborazione in corso, senza spegnere il computer e segnalare l'accaduto al personale del Servizio IT.

L'Utente è direttamente e totalmente responsabile dell'uso di Internet, delle informazioni che immette, delle modalità con cui opera, dei siti web o pagine internet ai quali abbia stabilito collegamento tramite link.

Qualora vengano attivati eventuali controlli da parte dell'Organizzazione, tenuto conto degli strumenti elettronici installati, avverranno come di seguito indicato:

- gli apparati in uso, (ad esempio tramite un sistema proxy server) tracceranno in modo anonimo la navigazione effettuata dagli utenti in merito ai siti rilevati;
- tale tracciamento potrà essere visualizzato solo dall'Amministratore di sistema;
- nel caso di un sospetto illecito, l'Amministratore di sistema potrà abilitare, previa comunicazione agli utenti, la tracciatura degli accessi con associazione utente –sito visitato;
- il controllo potrà essere effettuato per un massimo di 6 mesi, tempo massimo di conservazione anche dei log di navigazione.

L'Organizzazione periodicamente potrà effettuare controlli a campione sugli accessi internet effettuati dai dipendenti/collaboratori stessi.

Si rende noto che l'Organizzazione è autorizzata al trattamento in forma anonima, tale da precludere l'immediata identificazione degli utenti, dei dati relativi al "traffico" internet. I file di LOG verranno conservati per il tempo strettamente necessario al perseguimento di finalità organizzative, produttive e di sicurezza.

Verranno prolungati i tempi di conservazione (limitatamente comunque alle sole informazioni indispensabili per perseguire finalità preventivamente determinate) solo in caso di:

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

Il controllo anonimo potrebbe concludersi con un avviso generalizzato relativo ad un rilevato utilizzo anomalo degli strumenti aziendali e con l'invito ad attenersi scrupolosamente a compiti assegnati e istruzioni impartite.

Si ribadisce che i controlli rispettano i principi di pertinenza e di non eccedenza.

In nessun caso verranno compiuti controlli prolungati, costanti o indiscriminati.

I controlli saranno svolti in conformità alla legge, sia per eseguire verifiche sulla funzionalità e sicurezza del sistema, sia per verificare il corretto utilizzo da parte degli utenti (dipendenti, collaboratori etc.) tanto della rete Internet che della posta elettronica. Nell'esercizio del potere di controllo l'Organizzazione si atterrà al principio generale di proporzionalità e non eccedenza delle attività di controllo.

10. Principali minacce

Al fine di sensibilizzare gli utenti ad un uso diligente delle risorse messe a disposizione dall'Organizzazione, vengono indicate di seguito alcune minacce che rappresentano una fonte di rischio per l'intero sistema informativo:

Malware

Nella sicurezza informatica il termine malware indica genericamente un qualsiasi software creato con il solo scopo di causare danni più o meno gravi ad un computer, ai dati degli utenti del computer, o a un sistema informatico su cui viene eseguito.

Il termine deriva dalla contrazione delle parole inglesi malicious e software e ha dunque il significato letterale di "programma malvagio"; in italiano è detto anche codice maligno.

Si distinguono molte categorie di malware, anche se spesso questi programmi sono composti di più parti interdipendenti e rientrano pertanto in più di una classe. Vista inoltre la rapida evoluzione in questo campo, la classificazione presentata di seguito non è da ritenersi esaustiva.

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. Si trasmettono da un computer a un altro tramite lo spostamento di file infetti ad opera degli utenti.

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. Per indurre gli utenti ad eseguirli utilizzano tecniche di ingegneria sociale, oppure sfruttano dei difetti (bug) di alcuni programmi per diffondersi automaticamente. Il loro scopo è rallentare il sistema con operazioni inutili o dannose.

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.

CryptoLocker: una forma di ransomware infettante i sistemi Windows e che consiste nel criptare i dati della vittima, richiedendo un pagamento per la decriptazione. Cryptolocker generalmente si diffonde come allegato di posta elettronica apparentemente lecito e inoffensivo che sembra provenire da mittenti legittimi.

Backdoor: letteralmente "porta sul retro". Sono dei programmi che consentono un accesso non autorizzato al sistema su cui sono in esecuzione. Tipicamente si diffondono in abbinamento ad un trojan o ad un Worm, oppure costituiscono una forma di accesso lecita di emergenza ad un sistema, inserita per permettere ad esempio il recupero di una password dimenticata.

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.

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 tipo 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 spacciati anche a pagamento.

Rabbit: i rabbit sono programmi che esauriscono le risorse del computer creando copie di sé stessi (in memoria o su disco) a grande velocità.

Adware: programmi software che presentano all'utente messaggi pubblicitari durante l'uso, 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.

Batch: i Batch sono i cosiddetti "virus amatoriali". Non sono sempre dei file pericolosi in quanto esistono molti file batch tutt'altro che dannosi, il problema arriva quando un utente decide di crearne uno che esegua il comando di formattare il pc (o altri comandi dannosi) dell'utente a cui viene mandato il file. Non si apre automaticamente, deve essere l'utente ad aprirlo, perciò dato che l'antivirus non rileva i file Batch come pericolosi è sempre utile assicurarsi che la fonte che vi ha mandato il file sia attendibile oppure aprirlo con blocco note per verificare o meno la sua pericolosità. Bisogna però anche dire che esistono modi per camuffare i Batch e farli sembrare dei file exe, aumentandone anche il peso per sedare ogni sospetto. L'utilizzo di questo particolare "malware" è spesso ricorrente nel Cyberbullismo.

Keylogger: i Keylogger sono dei 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. La differenza con gli Adware sta nel fatto che il computer non si accorge della presenza del Keylogger e il programma non causa rallentamento del pc, passando così totalmente inosservato. Generalmente i Keylogger vengono installati sul computer dai trojan o dai Worm, in altri casi invece il Keylogger viene installato sul computer da un'altra persona che può accedere al pc o attraverso l'accesso remoto (che permette a una

persona di controllare un altro pc dal suo stesso pc attraverso un programma) oppure in prima persona, rubando così dati e password dell'utente.

Rogue antispyware: 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 dal cracker stesso.

Zip Bomb: è un file che si presenta come un file compresso. Deve essere l'utente ad eseguirlo. All'apparenza sembra un innocuo file da pochi Kilobyte ma, appena aperto, si espande fino a occupare tutto lo spazio su disco rigido.

Nell'uso comune il termine virus viene utilizzato come sinonimo di malware e l'equivoco viene alimentato dal fatto che gli antivirus permettono di rilevare e rimuovere anche altre categorie di software maligno oltre ai virus propriamente detti.

Intercettazioni delle comunicazioni: possono comportare l'accesso non autorizzato alle banche dati per consultazione e copia di dati personali da parte di persone non autorizzate.

Attacchi alle password: questi attacchi effettuati in varia forma sono dei tentativi per venire a conoscenza e quindi rubare le password degli utenti, di programmi e di accesso a siti Internet. Alcuni esempi sono i seguenti:

Brute Force: un apposito programma prova tutte le possibili combinazioni di chiavi per decrittare il file protetto.

Attacco a Dizionario: prova lunghissimi elenchi di parole, nomi e sigle di uso comune in una data lingua.

Attacco all'Algoritmo: prevede la possibilità di intervenire su particolari debolezze matematiche o computazionali dell'algoritmo utilizzato.

Password Sniffing: ruba la password - sniff - con qualche trucco, carpendola con un inganno ad esempio fingendosi responsabili di un servizio assistenza clienti o della sicurezza.

Crimini informatici: i sistemi informatici potrebbero essere utilizzati per compiere crimini informatici con implicazioni di tipo civile e penale (spamming, tentativi di intrusione, trattamento di testi o immagini proibite, violazione della corrispondenza, scaricamento di software o file non autorizzato o coperti da diritto d'autore, etc.).

Danni all'hardware: l'elemento più delicato dell'elaboratore è il disco fisso. Se si dovesse danneggiare, a meno di ricorrere a pratiche costosissime sviluppate da centri specializzati, tutti i dati andrebbero persi. Quindi è fondamentale la centralizzazione di tutti i dati sul server.

Usurpazione di identità: al momento di stabilire un collegamento alla rete o di ricevere dati, l'utente deduce l'identità del suo interlocutore in funzione del contesto in cui avviene la comunicazione e potrebbe scaricare un software maligno da un sito web che si fa passare per fonte affidabile per cui si potrebbero anche rivelare informazioni riservate alla persona sbagliata.

IP spoofing: l'autore dell'attacco sostituisce la propria identità a quella di un utente legittimo del sistema. Viene fatto non per generare intrusione in senso stretto, ma per effettuare altri attacchi. Lo spoofing si manifesta come attività di "falsificazione" di alcuni dati telematici, come ad esempio di un indirizzo IP o dell'indirizzo di partenza dei messaggi di posta elettronica.

Spamming: saturazione di risorse informatiche a seguito dell'invio di un elevato numero di comunicazioni tali da determinare l'interruzione del servizio. Ad esempio l'invio di molti messaggi di posta elettronica con allegati provoca la saturazione della casella e la conseguente non disponibilità a ricevere ulteriori messaggi.

Incidenti ambientali e eventi imprevisti: calamità naturali (tempeste, inondazioni, incendi e terremoti); guasti dell'hardware o del software dei componenti o dei programmi utilizzati; errore umano dell'operatore (compresi i fornitori di servizi) o dell'utente (ad esempio problemi di gestione della rete, installazione errata del software).

11. Comportamento da tener in caso di rilevazione anomalia o punto di debolezza del sistema informativo o indisponibilità dei dati

In caso di rilevazione di un'anomalia o punto di debolezza del sistema informativo, soprattutto se impatta o può potenzialmente impattare sulla sicurezza dei dati personali intesa come integrità, disponibilità e riservatezza, l'Utente è tenuto a darne tempestiva comunicazione, possibilmente scritta, al Responsabile opportunamente

individuato. L'utente deve inoltre collaborare attivamente con quest'ultimo, in base alle indicazioni ricevute, per la tempestiva risoluzione e per la verifica del ripristino delle condizioni di normalità.

In caso si verifichi una violazione dei dati personali (data breach), ossia una violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati è necessario darne immediata comunicazione al Responsabile della protezione dei dati, se individuato, o al Titolare, affinché possano attivare le procedure di notifica previste dalla legge.

12. Utilizzo di fax, stampanti e fotocopiatrici, telefoni, tablet

Il telefono o qualsiasi strumento di telefonia o connettività mobile affidato all'Utente è uno strumento di lavoro. Ne viene concesso l'uso esclusivamente per lo svolgimento dell'attività lavorativa, non essendo quindi consentite comunicazioni a carattere personale o comunque non strettamente inerenti l'attività lavorativa stessa. La ricezione o l'effettuazione di telefonate personali è consentito solo nel caso di comprovata necessità ed urgenza.

L'eventuale uso promiscuo (anche per fini personali) del telefono cellulare aziendale o di qualsiasi strumento di telefonia o connettività mobile affidato all'Utente è possibile soltanto in presenza di preventiva autorizzazione scritta e in conformità alle istruzioni al riguardo impartite dall'Organizzazione.

È vietato l'utilizzo dei fax dell'Organizzazione per fini personali, tanto per spedire quanto per ricevere documentazione, salva diversa esplicita autorizzazione da parte dell'Organizzazione.

Inserire a piè di pagina dei fax inviati la seguente dicitura:

> *"Questo messaggio fax è ad uso esclusivo del soggetto cui è indirizzato, e potrebbe contenere informazioni riservate. Se aveste ricevuto questo fax per errore, ci scusiamo per l'accaduto e Vi invitiamo cortesemente a darcene notizia e a distruggere il messaggio ricevuto. Vi ricordiamo, inoltre, che la comunicazione, la diffusione, l'utilizzo e/o la conservazione dei dati ricevuti per errore, costituiscono violazioni alle disposizioni del Regolamento Generale sulla protezione dei dati personali 679/2016 dell'Unione Europea e sono sanzionabili ai sensi dell'art. 616 del Codice Penale."*

È vietato l'utilizzo delle fotocopiatrici e delle stampanti dell'Organizzazione per fini personali, salvo preventiva ed esplicita autorizzazione di quest'ultima.

13. Accesso ai dati trattati dall'Utente

È facoltà dell'Organizzazione, tramite il personale incaricato della gestione del sistema informatico o addetti alla manutenzione, accedere direttamente, nel rispetto della normativa sulla *privacy*, a tutti gli strumenti informatici dell'Organizzazione e ai documenti ivi contenuti. Le informazioni raccolte mediante tali operazioni di accesso, sulla base del presente regolamento che funge anche da strumento informativo, possono essere utilizzate a tutti i fini connessi al rapporto di lavoro ai sensi dell'art. 4, comma 3, Legge 300/1970 (come modificato dal D.Lgs. 151/2015).

14. Indicazioni per il trattamento dei dati senza l'ausilio di strumenti elettronici

Al fine di ridurre il rischio di accesso non autorizzato ad informazioni aziendali, è necessario che l'Utente segua delle politiche di "scrivania pulita". Con tali termini si intende che l'Utente presti particolare attenzione a materiale cartaceo e dispositivi di memoria rimovibili.

Di conseguenza gli atti e i documenti contenenti dati personali comuni identificativi devono essere conservati nel rispetto di quanto segue:

- conservazione in archivi ad accesso selezionato;
- particolare attenzione posta alle stampe che, a volte, possono essere dimenticate sulle stampanti o ritirate dopo un tempo piuttosto lungo, lasciandole così incustodite e a disposizione di chiunque;
- l'Incaricato in caso di assenza - anche momentanea - dall'ufficio provvede a riporre la documentazione negli archivi;
- al termine del trattamento la documentazione deve essere restituita o distrutta se non sussiste l'esigenza di conservazione;

- la distruzione della documentazione deve essere effettuata in modo che non vi sia la possibilità di recupero e/o consultazione, e quindi sono da evitare cestini o contenitori per il riciclaggio della carta senza prima essersi assicurati dell'impossibilità del recupero del contenuto della documentazione;
- nel caso gli archivi contenenti dati personali siano ubicati in zona con accesso al pubblico, sono previsti armadi o contenitori muniti di serratura e sono predisposte "barriere" o distanze "di sicurezza" tali da impedire che soggetti non autorizzati possano visionare documenti durante il trattamento da parte degli Incaricati;
- non trasferire i documenti contenenti dati personali al di fuori dei locali preposti alla loro conservazione, se non in casi del tutto eccezionali.

In aggiunta, in caso di trattamento di dati personali sensibili e/o giudiziari o comunque critici:

- la documentazione deve essere conservata in luoghi ad accesso controllato e selezionato e custodita in archivi muniti di serratura (locali e armadi chiusi a chiave - anche elettronica, cassetti chiusi a chiave, casseforti, etc.);
- la documentazione contenente dati personali sensibili e/o giudiziari deve essere conservata separatamente rispetto alla documentazione cartacea contenente dati personali comuni identificativi.

In caso di utilizzo di fax e posta tradizionale, l'Utente deve inoltre osservare le seguenti indicazioni:

- per la gestione dei fax e le comunicazioni mediante posta tradizionale, possono essere individuati uno o più soggetti Incaricati al trattamento dei suddetti documenti;
- è cura dell'Incaricato smistare e consegnare i documenti alle persone o agli uffici competenti, evitando che il trattamento venga effettuato da persone non autorizzate;
- i documenti ricevuti per errore devono essere distrutti o restituiti al mittente senza essere diffusi e/o utilizzati.

15. Controlli

Al fine di verificare il corretto utilizzo degli strumenti come da prescrizioni esplicitate nel presente paragrafo potranno essere svolti dei controlli sia "remoti" (attraverso sistemi software all'uopo deputati) che "fisici" presso le singole postazioni o i singoli strumenti.

In nessun caso verranno compiuti controlli prolungati, costanti o indiscriminati.

I controlli saranno svolti in conformità alla legge, sia per eseguire verifiche sulla funzionalità e sicurezza del sistema, sia per verificare il corretto utilizzo da parte degli utenti (dipendenti, collaboratori etc.). Nell'esercizio del potere di controllo l'Organizzazione si atterrà al principio generale di proporzionalità e non eccedenza delle attività di controllo.

Il personale tecnico specificatamente incaricato è autorizzato a compiere interventi nel sistema informatico dell'Organizzazione ed ha la facoltà di collegarsi alle singole postazioni di lavoro al fine di garantire l'assistenza tecnica, la normale attività operativa e la sicurezza e salvaguardia del sistema stesso.

Il personale incaricato della gestione del sistema informatico può in qualunque momento procedere alla rimozione di ogni file o applicazioni installati in violazione delle prescrizioni di cui al presente regolamento.

Il personale incaricato della gestione del sistema informatico può in qualunque momento eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.

15.1. Sistemi di controllo graduali

L'organizzazione informa circa la necessità di porre in essere adeguati sistemi di controllo sull'utilizzo degli strumenti di cui al presente Regolamento nel rispetto dei criteri e dei principi stabiliti dal Garante per la protezione dei dati personali (provvedimento n. 13 del 01/03/07) e di valutare conseguentemente gli usi scorretti che, oltre ad esporre l'Organizzazione stessa a rischi, tanto patrimoniali quanto penali, possono di per sé considerarsi contrari ai doveri di diligenza e fedeltà previsti dagli artt. 2104 e 2105 del Codice Civile.

I controlli sull'uso degli strumenti informatici/telefonici tuttavia garantiranno tanto il diritto di proteggere la propria Organizzazione, essendo strumenti di lavoro la cui utilizzazione personale è preclusa, quanto il diritto del lavoratore a non vedere invasa la propria sfera personale, e quindi il diritto alla riservatezza ed alla dignità come sanciti dallo Statuto dei lavoratori (legge n. 300/1970) e dal General Data Protection Regulation - GDPR (Regolamento 679/2016/UE).

Il Regolamento, essendo rilevante ai fini delle eventuali azioni disciplinari attivabili dal datore di lavoro nei confronti del dipendente, è stato redatto tenendo opportunamente conto altresì delle disposizioni contenute nella Legge. n. 300/1970 in tema di provvedimenti disciplinari.

Nel rispetto della normativa in tema di protezione dei dati personali, l'attività di controllo espletata dall'Organizzazione garantisce il rispetto dei principi fondamentali di "proporzionalità", i diritti e le libertà fondamentali, nonché la dignità dell'interessato e soprattutto prevede la fornitura di un'adeguata e preventiva informativa.

Si comunica pertanto che in caso di anomalie, il personale incaricato dalla Direzione potrà effettuare controlli anonimi, che si concluderanno con avvisi generalizzati diretti ai dipendenti dell'area / settore in cui è stata rilevata l'anomalia, nei quali si evidenzierà l'utilizzo irregolare degli strumenti aziendali e si inviteranno gli interessati ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite.

In nessun caso verranno compiuti controlli prolungati, costanti o indiscriminati.

16. Sanzioni

È fatto obbligo a tutti gli utenti di osservare le disposizioni portate a conoscenza con il presente Regolamento. Il mancato rispetto o la violazione delle regole sopra ricordate è perseguibile nei confronti del personale dipendente con provvedimenti disciplinari e risarcitori previsti dal vigente C.C.N.L. applicabile, nonché con tutte le azioni civili e penali consentite anche nei confronti di collaboratori e professionisti.

17. Entrata in vigore, riesame e aggiornamento

Il presente regolamento è in vigore a partire dal 21/05/2022.

Il Regolamento viene riesaminato ed aggiornato con cadenza periodica o nel caso in cui si siano verificati cambiamenti significativi, al fine di garantirne sempre l'idoneità, l'adeguatezza e l'efficacia.