Camera di Commercio
Caserta

Unità Organizzativa Segreteria generale, RR.UU.
PEC: camera.commercio.caserta@ce.legalmail.camcom.it

COMUNICAZIONE DI SERVIZIO DEL 11.10.2018

OGGETTO: Piano di prevenzione della corruzione 2018-2020 – Sicurezza informatica

Premessa

La sicurezza informatica è un elemento sempre più rilevante nell'ambito delle moderne organizzazioni, sia pubbliche che private, soprattutto in seguito alla maggior interconnessione dei sistemi ed il considerevole aumento dei servizi offerti attraverso la rete Internet. Il proliferare e l'aumento del numero e della varietà dei dispositivi connessi alla rete, rende, infatti, sempre più complesso avere una puntuale gestione della sicurezza informatica anche a causa di un elevato flusso di dati continuamente crescente e spesso ingestibile sotto il profilo della protezione delle risorse e delle informazioni aziendali.
Il corrente Piano Triennale di prevenzione della corruzione adottato dalla Camera, tiene conto della rilevanza del tema della security policy, individuandolo tra gli obiettivi dell'ente per il 2018, attraverso l'elaborazione di specifiche linee guida che dovranno, in seguito, essere ulteriormente dettagliate, al fine di armonizzarle con quanto previsto in tema di protezione dei dati personali.
L'attuale rilevanza del tema della sicurezza può essere, infatti, colta anche nel vigente quadro normativo in materia di tutela della riservatezza e di protezione dei dati personali. Il nuovo Regolamento Europeo 2016/679 in materia di protezione dei dati personali, in vigore dal 25 maggio scorso, prevede (art.32) l'obbligo di garantire l'osservanza di adeguate misure di sicurezza, indifferentemente dalla natura del supporto contenete dati personali, tenendo conto dello stato dell'arte, dei costi di realizzazione, dell'oggetto e del contesto e delle finalità del trattamento. Misure che il testo regolamentare individua, a titolo esemplificativo, nelle seguenti:

- la pseudonimizzazione e la cifratura dei dati personali;
- la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
- la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
- una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Nel valutare l'adeguato livello di sicurezza, si deve tenere conto, in special modo, dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

La sicurezza informatica

Per sicurezza informatica si intende il complesso dei mezzi e delle tecnologie tesi alla protezione dei sistemi informatici in termini di disponibilità, confidenzialità, integrità ed autenticità delle informazioni. Assicurare la protezione di un sistema informatico significa, quindi, preservare le sue risorse dall'uso non autorizzato e salvaguardare le informazioni in esso contenute da letture o manipolazioni non autorizzate, accidentali o deliberate.
Un sistema è sicuro se riesce a garantire i seguenti tre obiettivi:

- **Disponibilità** dei dati, ossia salvaguardia del patrimonio informativo nella garanzia di accesso, usabilità e confidenzialità dei dati. Da un punto di vista di gestione della sicurezza significa ridurre a livelli accettabili i rischi connessi all'accesso alle informazioni (intrusioni, furto di dati, ecc.).
- **Integrità** dei dati, intesa come garanzia che l'informazione non subisca modifiche o cancellazioni a seguito di errori o di azioni volontarie, ma anche a seguito di malfunzionamenti o danni dei sistemi tecnologici.
- **Riservatezza** informatica cioè gestione della sicurezza in modo tale da mitigare i rischi connessi all'accesso o all'uso delle informazioni in forma non autorizzata

Ciò premesso, possiamo, quindi, confermare l' impegno dell'ente camerale per garantire efficaci politiche di sicurezza, con l'individuazione delle relative misure di sicurezza, intendendo per politiche di sicurezza informatica le linee guida di carattere generale che devono essere seguite nel progetto, nella implementazione e nella gestione dell'ambiente informatico, e per misure di sicurezza i meccanismi e il complesso di prescrizioni, di carattere organizzativo e comportamentale, da adottare al fine di minimizzare il danno. Di seguito vengono dettagliate le prescrizioni di sicurezza che ciascun dipendente e tutti i soggetti che, a qualunque titolo, prestino la propria collaborazione in favore e presso la camera di commercio, sono tenuti ad osservare.

Le misure di sicurezza

1. Gestione strumenti elettronici

Ciascun dipendente è responsabile del corretto utilizzo e della custodia degli strumenti elettronici in dotazione (a titolo esemplificativo personal computer, periferiche, lettori di smart card).

Al termine dell'orario di lavoro, il PC deve essere spento, a meno che non stia svolgendo elaborazioni particolari. In tal caso gli uffici debbono essere chiusi a chiave.

In caso di allontanamento temporaneo dalla propria postazione di lavoro, è necessario accertarsi che il proprio pc non sia accessibile da altri soggetti. In particolare, bisogna chiudere la sessione di lavoro sul PC facendo Logout, oppure attivare la procedura di blocco, protetto dalle credenziali di autenticazione;

Relativamente all'eventuale utilizzo dello screen-saver, occorre osservare le seguenti norme:

- Non deve mai essere disattivato;
- Il suo avvio automatico deve essere previsto non oltre i primi 10 minuti di inattività del PC.

Il dipendente ha divieto di utilizzare il cellulare o altri dispositivi personali sulla rete camerale per non mettere a rischio gli strumenti informatici dell'ente, al fine di garantire la massima sicurezza del sistema.

Il dipendente ha obbligo di segnalare al referente informatico qualsiasi episodio anomalo, anche occasionale, che si verifichi al proprio pc.

I supporti magnetici od ottici contenenti dati personali devono essere cancellati prima di essere riutilizzati. Se ciò non è possibile, essi devono essere distrutti secondo modalità che ne impediscano la ricomposizione.

2.Gestione username e password

L'accesso al PC, sia esso collegato in rete o meno, è protetto da un sistema di autenticazione che richiede all'utilizzatore di inserire sulla videata di accesso all'elaboratore un codice utente (username), associato ad una parola chiave (password). L'adozione ed il corretto utilizzo della combinazione username / password è fondamentale per la sicurezza informatica.

Per quanto concerne la scelta:

- la password deve avere lunghezza non inferiore ad otto caratteri, contenendo una combinazione di numeri e/o segni speciali, lettere, maiuscole e minuscole;
- non deve essere uguale alle precedenti

Per quanto concerne la corretta gestione della parola chiave:

- è necessario modificarla al primo utilizzo;
- non rivelarla o condividerla con colleghi di lavoro, parenti e amici, e soprattutto attraverso il telefono.
- non memorizzare la password sulle diverse applicazioni informatiche personali né lasciarle scritte su etichette accessibili a tutti;
- non utilizzarle per applicazioni informatiche personali e cambiarle periodicamente, qualora il sistema non imponga, automaticamente, il cambio password periodico.
- Non utilizzare la funzione, offerta da alcuni software, di salvare automaticamente la password per successivi utilizzi delle applicazioni.

Va precisato che gli applicativi in uso, gestiti da Infocamere, prevedono, semestralmente, il cambio della password.

I responsabili delle unità organizzative sono tenuti ad effettuare una verifica periodica delle abilitazioni ai diversi servizi del sistema informatico camerale in uso dai propri collaboratori. In particolare, i responsabili delle unità organizzative dovranno comunicare al referente informatico dell'ente le abilitazioni occorrenti al personale di nuova assegnazione, chiedendo, tempestivamente, la disattivazione delle credenziali di coloro che, per qualsiasi motivo, non siano addetti più alle funzioni per le quali le credenziali erano state assegnate.

In caso di assenza od impedimento dell'incaricato e contestuale esigenza di accedere ai dati detenuti presso banche dati o p.c. in uso all'incaricato, il referente informatico, su richiesta del responsabile dell'unità organizzativa, deve attivare procedure di accesso temporaneo, mediante generazione di nuove credenziale di autenticazione. Le nuove credenziali di autenticazioni devono essere disattivate al termine della sessione straordinaria di lavoro.

3.Installazione di hardware e software

L'installazione di hardware e software, nonché la modifica dei parametri di configurazione, possono essere eseguiti solamente dal Referente informatico su autorizzazione del Responsabile dell'Unità Organizzativa, sentito il Responsabile del trattamento. E' necessario assicurare che i dipendenti non installino sulla postazione di lavoro programmi non attinenti alle attività di ufficio, ovvero programmi senza la preventiva autorizzazione. I Responsabili delle unità organizzative, qualora non siano in grado di apprezzare l'impatto dei programmi per i quali si è chiesta l'installazione, si coordinano con il referente informatico dell'Ente per concordare la linea di condotta. Pertanto si raccomanda agli utenti dei PC di rispettare le seguenti indicazioni:

• Non utilizzare sul PC dispositivi personali, o comunque non aziendali, quali lettori dispositivi di memorizzazione dei dati;

• Non installare sistemi per connessione esterne (es : modem, wifi); tali connessioni, aggirando i sistemi preposti alla sicurezza della rete aziendale, aumentano sensibilmente i rischi di intrusioni e di attacchi dall'esterno;

• Non installare programmi, anche in versione demo. In particolare, è vietata l'installazione di giochi, programmi in prova (shareware), programmi gratuiti (freeware), programmi pirata, e in generale tutti i software non autorizzati dal Servizio Informatico;

L'aggiornamento automatico dei software in uso viene effettuata periodicamente da Infocamere.

La condivisione di aree e di risorse del proprio PC viene effettuata dal referente informatico, su richiesta del responsabile dell'unità organizzativa. In questi casi devono essere adottate password di lettura e scrittura e la condivisione deve operare solo su singole directory del PC, e non sull'intero disco rigido.

4.Gestione posta elettronica aziendale

Il servizio di posta elettronica è funzionale rispetto alle attività e alle mansioni svolte dai dipendenti, in relazione alle finalità dell'Ente e in stretta connessione con l'effettiva attività e mansioni del dipendente che utilizza tale funzionalità.

Al fine di non compromettere la sicurezza dell'Ente e di prevenire possibili conseguenze legali è necessario adottare le seguenti norme comportamentali:

- È fatto divieto di utilizzare le caselle di posta elettronica per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail list, salvo diversa ed esplicita autorizzazione;
- Procedere alla immediata eliminazione di mail provenienti da destinatari sconosciuti contenenti file di qualsiasi tipo;
- Tenere in ordine la propria casella di posta elettronica, eliminando i documenti inutili;
- quando si riceve un link di collegamento, non cliccare sul link ma riscriverlo sulla barra dell'indirizzo oppure scriverlo sul motore di ricerca. Ciò al fine di evitare che detto link possa consentire il collegamento ad una piattaforma indesiderata o illecita.

5.Gestione del salvataggio dei dati

a) Per dati e documenti che risiedono esclusivamente sul PC, ogni addetto deve effettuare periodicamente il back up dei dati registrati sul proprio PC sulle apposite cartelle collocate nell'area utenti del server. Questo allo scopo di garantire la disponibilità ed il ripristino dei Dati Personali nel caso di una generica compromissione delle risorse (cancellazioni accidentali, guasti, furti…) e per evitare rischi che soggetti terzi possano crittografare i dati e farne uso illecito.

b) Per dati e documenti che risiedono sui server gestiti centralmente, come ad esempio cartelle di rete e database, il back-up dei dati viene effettuato centralmente da InfoCamere (il Servizio Informatico) con la possibilità di ripristinare in toto oppure selettivamente eventuali files distrutti, ad esempio per guasti hardware oppure per cancellazioni involontarie.

c) Per quanto concerne, in particolare, la posta elettronica, in considerazione della circostanza che il nuovo client di posta elettronica in uso presso l'ente è Gmail, l'incaricato può effettuare le operazioni di salvataggio

dei dati, utilizzando le app messe a disposizione da Google (ad esempio Drive).

6.Gestione protezione dai virus informatici

Per prevenire eventuali danneggiamenti al software causati dalla presenza o dall'azione di programmi virus informatici, in fase di predisposizione della postazione di lavoro viene installato l'antivirus, che viene aggiornato, a livello centrale, da InfoCamere. L'antivirus aziendale non deve mai essere disattivato o sostituito con altro antivirus non ufficialmente fornito.

Nel caso il programma antivirus installato sul proprio PC riscontri la presenza di un virus, oppure si sospetti la presenza di un virus non rilevato dal programma antivirus è necessario darne immediatamente segnalazione al Referente Informatico.

Si raccomanda di non scaricare e né tantomeno aprire file provenienti via e-mail da mittenti sconosciuti. Tali file, possono essere portatori di virus e compromettere la funzionalità del PC, l'integrità dei dati in essa contenuti e soprattutto l'integrità dei sistemi collegati al PC stesso.

Per quanto concerne la posta elettronica, il client utilizzato dalla Camera "GMail", cancella automaticamente gli allegati ritenuti sospetti. In ogni caso, al fine di non aumentare il livello di rischio di contaminazione da virus è opportuno che i dipendenti provvedano a:

1 verificare che sul computer sia sempre operativo il programma antivirus aggiornato e con la funzione di monitoraggio attiva;

2 accertarsi sempre della provenienza dei messaggi di posta elettronica contenenti allegati; nel caso che il mittente dia origine a dubbi, cancellare direttamente il messaggio senza aprire gli allegati

3 non scaricare da Internet programmi o file non inerenti l'attività lavorativa o comunque sospetti.

Osservanza delle prescrizioni

I Dirigenti, coadiuvati dai Responsabili delle unità organizzative, sono tenuti a vigilare sul rigoroso rispetto delle prescrizioni fornite in questa sede, nonché a proporre eventuali ed ulteriori misure ritenute necessarie ed opportune per la sicurezza informatica.

Le presenti disposizioni integrano elementi di valutazione della condotta del lavoratore. La violazione delle prescrizioni contenute può generare, oltre che responsabilità penali e civili, l'irrogazione di sanzioni disciplinari, in considerazione della gravità della condotta.

Caserta, 11 ottobre 2018

IL SEGRETARIO GENERALE
Luca Perozzi

Camera di Commercio Industria Artigianato ed Agricoltura di Caserta
Via Roma, 75 – 81100 Caserta - Tel: 0823.249111 – Fax 0823.249299
PEC: camera.commercio.caserta@ce.legalmail.camcom.it
e-mail: info@ce.camcom.it sito web: www.ce.camcom.it
C.F.: 80004270619 P. I.: 00908580616