CAMERA DI COMMERCIO
IRPINIA SANNIO

LINEE GUIDA

MISURE DI SICUREZZA DEGLI STRUMENTI INFORMATICI

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.

2.Gestione username e password

L'accesso al PC, 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, periodicamente, il cambio della password.

I Dirigenti 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.

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 Dirigente.. 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 Dirigenti,, 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;

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

La condivisione di cartelle di aree del server viene effettuata da Infocamere dietro richiesta del referente Informatico, mentre eventuali nuove risorse del proprio PC, prima di essere installate vanno valutate dal referente informatico per poi eventualmente essere installate sul PC fisico, su richiesta del Dirigente.

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

I dati e i documenti risiedono su server gestiti centralmente. Il back-up dei dati viene pertanto 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.

6.Gestione protezione dai virus informatici

Per prevenire eventuali danneggiamenti al software causati dalla presenza o dall'azione di programmi virus informatici, è presente l'antivirus, che viene aggiornato, a livello centrale, da InfoCamere..

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.

IL SEGRETARIO GENERALE
Dott. Luca Perozzi