

# Documento Programmatico sulla Sicurezza

(D. Lgs. n. 196/2003 “Codice in materia di Protezione dei Dati Personali”)

<b>1. Introduzione al Documento .....</b>	<b>3</b>
1.1 Novità introdotte rispetto alla precedente emissione .....	3
1.2 Scopo e campo di applicazione del documento.....	4
1.3 Riferimenti .....	4
1.4 Termini e definizioni .....	4
<b>2. Il Documento Programmatico .....</b>	<b>6</b>
2.1 Disciplinare tecnico .....	6
2.2 Elenco dei Trattamenti .....	6
2.3 Compiti e Responsabilità.....	7
2.4 Analisi dei Rischi .....	7
2.5 Sicurezza Fisica e Sicurezza Logica.....	7
2.6 Ripristino dei dati.....	8
2.7 Interventi formativi .....	9
2.8 Trattamenti affidati all'esterno .....	9

## 1. Introduzione al Documento

L' 1 gennaio 2004 è entrato in vigore il nuovo "Codice in Materia di Protezione dei Dati Personali" (approvato con Decreto Legislativo 30 giugno 2003, n. 196) che sostituisce ogni altra norma in tema di privacy.

Tale Codice ribadisce il principio che i dati personali oggetto di trattamento debbano essere custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta (cfr. art.31).

Nel quadro dei più generali obblighi di sicurezza sopra descritti o previsti da speciali disposizioni, i titolari del trattamento sono comunque tenuti ad adottare misure di sicurezza volte ad assicurare un livello adeguato di protezione dei dati personali.

Il trattamento di dati personali è consentito solo se sono adottate le seguenti misure di sicurezza minime, nei modi previsti dall'apposito disciplinare tecnico.

- Autenticazione informatica;
- Adozione di procedure di gestione delle credenziali di autenticazione;
- Utilizzazione di un sistema di autorizzazione;
- Aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;
- Protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;
- Adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;
- [*Tenuta di un aggiornato Documento Programmatico sulla Sicurezza*]\*

\*Dal 10 febbraio 2012 non è più obbligatorio adottare e quindi tenere aggiornato tale Documento a seguito dell'abolizione dello stesso prevista dall'art. 45 del decreto-legge n. 5 del 9 febbraio 2012 ("Disposizioni urgenti in materia di semplificazione e di sviluppo").

In particolare tale decreto-legge ha soppresso:

- la lettera g) dell'art. 34, comma 1 del D.Lgs. n. 196/2003 (che prevedeva, tra le varie misure minime, l'adozione del DPS);
- i paragrafi da 19 a 19.8 del Disciplinare Tecnico costituente l'allegato B al D.Lgs. n. 196/2003 (che prevedevano i contenuti che doveva avere il DPS);
- il paragrafo 26 del Disciplinare Tecnico costituente l'allegato B al D.Lgs. n. 196/2003 (che prevedeva l'obbligo, per i titolari del trattamento, di riferire nella relazione accompagnatoria al bilancio di esercizio dell'avvenuto aggiornamento del DPS).

### 1.1 Novità introdotte rispetto alla precedente emissione

<b>Versione/Release n° :</b>	2.6	<b>Data Versione/Release :</b>	23/03/2012
<b>Descrizione modifiche:</b>	Aggiornamento del Documento Programmatico sulla Sicurezza		
<b>Motivazioni :</b>	Aggiornamento Banche Dati e Analisi dei Rischi		

## 1.2 Scopo e campo di applicazione del Documento

Nonostante l'intervenuta abrogazione del Documento Programmatico sulla Sicurezza da parte dell'art. 45 del Decreto-Legge n. 5 del 9.02.2012, rimane comunque fermo l'obbligo, a carico del Titolare, di adottare le altre misure minime di sicurezza, previste dal sopra citato Decreto Legislativo n. 196/2003.

Pertanto, anche se la tenuta di tale Documento, ad oggi, non è più obbligatoria né più sanzionata, è bene comunque tenere l'elenco delle disposizioni prese, che può tornar utile specie in caso di contestazioni.

Quindi il Documento che segue risponde ad una necessità pratica di riepilogare le attività svolte dall'Ente camerale in materia di misure di sicurezza.

## 1.3 Riferimenti

- [1] Decreto Legislativo n. 196/2003 e successive modifiche ed integrazioni ("Codice in materia di Protezione dei Dati Personali")

## 1.4 Termini e definizioni

"autenticazione informatica"

l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità;

"credenziali di autenticazione"

i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica;

"sistema di autorizzazione"

l'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente;

"trattamento"

qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati;

"dato personale"

qualunque informazione relativa a persona fisica, *[persona giuridica, ente od associazione]\**, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;

"dati identificativi"

i dati personali che permettono l'identificazione diretta dell'interessato;

"dati sensibili"

i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;

"dati giudiziari"

i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del D.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi

carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del Codice di Procedura Penale;

"titolare"	la persona fisica, la persona giuridica, la Pubblica Amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza;
"responsabile"	la persona fisica, la persona giuridica, la Pubblica Amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali;
"incaricati"	le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;
"interessato"	la persona fisica, [ <i>la persona giuridica, l'ente o l'associazione</i> ]* cui si riferiscono i dati personali;
"comunicazione"	il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
"diffusione"	il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
"banca di dati"	qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti.

---

\*soppresse dal comma 2 dell'art. 40 del D.L. n. 201 del 6.12.2011 convertito con modificazioni nella Legge n. 214 del 22.12.2011

## **2. Il Documento Programmatico**

### **2.1 Disciplinare tecnico**

Il presente Documento Programmatico sulla Sicurezza contiene idonee informazioni riguardo:

1. l'elenco dei trattamenti di dati personali;
2. la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;
3. l'analisi dei rischi che incombono sui dati;
4. le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;
5. la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento di cui al successivo punto 23 (dell'Allegato B, n.d.r);
6. la previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare. La formazione è programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali;
7. la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare;
8. per i dati personali idonei a rivelare lo stato di salute e la vita sessuale di cui al punto 24 (dell'Allegato B, n.d.r), l'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato.

Ciascun punto verrà ripreso ed approfondito nel seguito, ad esclusione del punto 8. che riguarda esclusivamente gli organismi sanitari e gli esercenti le professioni sanitarie.

### **2.2 Elenco dei Trattamenti**

L'elenco delle banche dati e dei trattamenti di dati personali effettuati dalla Camera di Commercio, direttamente o attraverso collaborazioni esterne, è individuato nel documento "Banche dati e Trattamenti di Dati Personali", parte del sistema di qualità della Camera.

In tale documento è evidenziato per ogni banca dati/trattamento l'ufficio che effettua il trattamento, il tipo di supporto (cartaceo o informatico), la presenza di dati sensibili, di dati giudiziari, il fatto che si tratti di un trattamento concernente funzioni istituzionali, l'eventuale comunicazione dei dati ad altri soggetti pubblici o privati.

Tale documento è aggiornato ad ogni nuovo trattamento ed è comunque verificato annualmente.

### **2.3 Compiti e Responsabilità**

I trattamenti di dati personali consentiti a ciascun collaboratore della Camera di Commercio – a prescindere dal tipo di contratto (a tempo determinato o indeterminato) e dalla qualifica – sono i trattamenti previsti all'interno dell'ufficio o del servizio in cui il collaboratore presta la propria opera. Tali trattamenti sono indicati nel documento “Banche dati e Trattamenti di Dati Personali”, rinvenibile nel sistema di qualità.

La preposizione della persona fisica ad uno specifico ufficio è definita dall'organigramma, parte del sistema di qualità, integrato da eventuali ordini di servizio.

La scelta di definire in questo modo gli incaricati dei trattamenti di dati personali è suggerita dall'articolo 30 del nuovo codice della privacy: *“Le operazioni di trattamento possono essere effettuate solo da incaricati che operano sotto la diretta autorità del titolare o del responsabile, attenendosi alle istruzioni impartite. La designazione deve essere effettuata per iscritto e individua puntualmente l'ambito del trattamento consentito. Si considera tale anche la documentata preposizione della persona fisica ad una unità per la quale è individuato, per iscritto, l'ambito del trattamento consentito agli addetti all'unità medesima.”*

### **2.4 Analisi dei Rischi**

L'elenco degli eventi potenzialmente dannosi per la sicurezza dei dati, la valutazione delle possibili conseguenze dell'accadimento di un evento dannoso, la valutazione della sua gravità e la correlazione con le contromisure previste costituiscono il contenuto del documento “Analisi dei Rischi della Camera di Commercio di Treviso”.

Tale documento contiene l'elenco degli eventi che possono generare danni e che comportano quindi rischi per la sicurezza dei dati personali. L'elenco identifica pertanto diversi eventi che possono avere una rilevanza per l'analisi dei rischi per la sicurezza dei dati personali. Contiene inoltre la descrizione delle principali conseguenze individuate per la sicurezza dei dati, in relazione a ciascun evento ed una valutazione della gravità delle stesse, anche in relazione alla probabilità stimata dell'evento.

Tale documento fa parte del sistema di qualità ed è rivisto annualmente.

### **2.5 Sicurezza Fisica e Sicurezza Logica**

Il furto o il danneggiamento delle apparecchiature informatiche, la diffusione o distruzione non autorizzata di informazioni personali e l'interruzione dei processi informatici possono esporre la Camera e InfoCamere al rischio di violare la legge.

Per tale motivo sono definite regole, emanate con appositi ordini di servizio, e istituiti controlli allo scopo di:

- limitare l'accesso fisico ad alcune aree - in modo particolare a quei locali che contengono apparecchiature informatiche critiche
- gestire correttamente i supporti di memorizzazione che contengono informazioni personali, in modo particolare se contengono dati sensibili o giudiziari
- garantire che il trattamento di dati personali con strumenti elettronici sia consentito solo agli incaricati dotati di credenziali di autenticazione nel rispetto delle misure di sicurezza previste dal codice della privacy in materia di autenticazione informatica e autorizzazione.

## 2.6 Ripristino dei dati

La maggior parte delle banche dati su supporto informatico sono gestite dalle società del sistema camerale Infocamere, Retecamere, Infocert e da Unioncamere nazionale, che gestiscono le procedure in modo da assicurare l'integrità delle banche dati e garantiscono il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento dei medesimi a seguito di errori software o di guasti hardware.

Per le banche dati non gestite dai soggetti sopra citati, sono indicati nella seguente tabella il nome della banca dati, la presenza di dati sensibili o giudiziari, la descrizione della tipologia di salvataggio e della frequenza con cui viene effettuato, l'indicazione del luogo fisico in cui sono custodite le copie dei dati salvate, la funzione aziendale della persona incaricata di effettuare il salvataggio e/o di controllarne l'esito.

Banca dati	Dati sens/giudiz.	Frequenza di salvataggio	Ubicazione copie	Responsabile
Web sibot	No	Giornaliera (max 30 gg ante)	Locale tecnico	Amministratore di sistema
Storico dei Verificatori impianti	Si	Giornaliera (max 30 gg ante)	Locale tecnico	Amministratore di sistema
Archimede	No	Giornaliera (max 30 gg ante)	Locale tecnico	Amministratore di sistema
Storico del Registro Sanzioni Upica	Si	Giornaliera (max 30 gg ante)	Locale tecnico	Amministratore di sistema
Data base posta elettronica	Si	Real Time + Giornaliera (max 30 gg ante)	Locale tecnico	Amministratore di sistema
Atti ed archivi di files degli uffici	Si	Giornaliera (max 30 gg ante)	Locale tecnico	Amministratore di sistema
Elenco dei fornitori/contratti	No	Giornaliera (max 30 gg ante)	Locale tecnico	Amministratore di sistema
Storico dei Molini e panifici	Si	Giornaliera (max 30 gg ante)	Locale tecnico	Amministratore di sistema
Archivio stipendi per controllo di gestione	No	Giornaliera (max 30 gg ante)	Locale tecnico	Amministratore di sistema
Banche dati concorsi uff. agricoltura	No	Giornaliera (max 30 gg ante)	Locale tecnico	Amministratore di sistema
Banche dati albi agricoltura	No	Giornaliera (max 30 gg ante)	Locale tecnico	Amministratore di sistema
Indirizzari vari in vari uffici	No	Giornaliera (max 30 gg ante)	Locale tecnico	Amministratore di sistema
Banca dati concorsi ufficio Industria	No	Giornaliera (max 30 gg ante)	Locale tecnico	Amministratore di sistema

Banca dati affluenza sportello industria	No	Giornaliera (max 30 gg ante)	Locale tecnico	Amministratore di sistema
Banche dati ufficio personale	Si	Giornaliera (max 30 gg ante)	Locale tecnico	Amministratore di sistema
Sito internet camerale (copia)	No	Giornaliera (max 30 gg ante)	Locale tecnico	Amministratore di sistema
Gettoni presenze (Uff. ragioneria)	No	Giornaliera (max 30 gg ante)	Locale tecnico	Amministratore di sistema
Banca dati ufficio affari generali – pareri legali	Si	Giornaliera (max 30 gg ante)	Locale tecnico	Amministratore di sistema
Sito Intranet	No	Giornaliera (max 30 gg ante)	Locale tecnico	Amministratore di sistema
Banca dati centralino telefonico (VOIP) (copia)	No	Giornaliera (max 30 gg ante)	Locale tecnico	Amministratore di sistema
Banca dati sistema rilevazione presenze (Timeweb)	No	Giornaliera (max 30 gg ante)	Locale tecnico	Amministratore di sistema
Banca Dati RI – circolari e informative	No	Giornaliera (max 30 gg ante)	Locale tecnico	Amministratore di sistema

## 2.7 Interventi formativi

Sono previsti interventi formativi per gli incaricati dei trattamenti, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime di sicurezza adottate dalla Camera di Commercio.

## 2.8 Trattamenti affidati all'esterno

Il quadro sintetico delle attività trasferite a terzi che comportano il trattamento di dati personali è di nuovo rinvenibile nel documento “Banche dati e Trattamenti di Dati Personali”.

In caso di trattamenti di dati personali che la Camera di Commercio affida all'esterno devono essere previste apposite clausole contrattuali riguardanti l'attuazione del codice della privacy, che garantiscano che il soggetto cui sono affidati i trattamenti:

- sia consapevole che i dati che tratterà nell'espletamento dell'incarico ricevuto sono dati personali e, come tali, sono soggetti all'applicazione del codice per la protezione dei dati personali;
- ottemperi agli obblighi previsti dal Codice per la Protezione dei Dati Personali;
- adotti misure di sicurezza non inferiori a quella adottate dalla Camera di Commercio;

- adottare le istruzioni specifiche eventualmente ricevute per il trattamento dei dati personali o le integrare nelle procedure già in essere;
- allertare immediatamente la Camera di Commercio in caso di situazioni anomale o di emergenze;
- riconoscere il diritto a verificare periodicamente l'applicazione delle norme di sicurezza adottate e a relazionare, su richiesta, sulle misure di sicurezza adottate.

## Analisi dei rischi della Camera di Commercio di Treviso

### Premessa

Il presente documento viene redatto conformemente a quanto previsto dal decreto legislativo n.° 196/2003 e successive modifiche ed integrazioni e richiamato nel documento programmatico della sicurezza della Camera di Commercio di Treviso.

Il documento contiene l'elenco degli eventi che possono generare danni agli archivi informatici e che possono potenzialmente comportarne quindi rischi per la sicurezza dei dati personali contenuti negli stessi.

### Obiettivi

Scopo del documento è individuare i rischi a cui il sistema informatico della Camera di Commercio di Treviso è sottoposto e prevedere le attività da svolgersi per prevenirli e le procedure per garantire la salvaguardia dei dati e le funzionalità del sistema informatico che consentono il trattamento dei dati stessi.

### Analisi della rete della Camera di Commercio di Treviso

La Camera di Commercio di Treviso è dotata di una rete informatica privata con punti di collegamento con l'esterno forniti esclusivamente da InfoCamere che ne garantisce la sicurezza.

Le strutture della rete locale sono ubicate in locali presidiati e chiuse in armadi non accessibili da persone non autorizzate. I Server sono ubicati in apposito locale sempre chiuso e l'accesso è consentito solo a persone preventivamente autorizzate e/o accompagnate da persone autorizzate.

Le stazioni di lavoro collegate alla rete camerale sono ubicate in locali presidiati e sono assegnate ad ogni dipendente che ne ha in carico la custodia e la salvaguardia.

Anche gli apparati telefonici, ora in VoIP, sono collegati al sistema di rete della Camera e sono ubicati negli stessi locali delle stazioni di lavoro ed in genere assegnati ad ogni dipendente che ne ha in carico generalmente la custodia e la salvaguardia.

### Individuazione delle responsabilità

Il documento programmatico della sicurezza della Camera di Commercio di Treviso provvede alla individuazione delle responsabilità ai fini della sicurezza e della salvaguardia dei dati e degli strumenti con cui sono trattati.

### Rischi individuati

#### Rischi fisici

- Furto o sottrazione
- Danni:
  - o Incendio
  - o Interruzioni di energia elettrica
  - o eventi calamitosi naturali ed umani

#### Rischi logici

- Accessi non autorizzati
- Virus, worm, spyware, malware
- Attacchi esterni ed interni ai sistemi informatici
- Vulnerabilità di sistema

### Conseguenze e gravità del rischio individuato

Rischi fisici	Conseguenze (ai fini del trattamento dei dati d.lgs. 196/2003)	Gravità	Probabilità
Furto o sottrazione			
<ul style="list-style-type: none"> <li>- attrezzature di lavoro workstation</li> <li>- server</li> </ul>	<p>Tutti i dati sono contenuti sui server camerali pertanto l'evento non comporta perdita di dati. Possono però essere scoperte informazioni sulle configurazioni delle macchine e della rete.</p> <p>Il furto dei server interromperebbe il servizio fino alla messa in opera di nuovi server; i dati sono salvaguardati dalle copie di sicurezza.</p> <p>I dati sensibili sono crittografati</p>	<p>Grave</p> <p>Molto grave</p>	<p>Molto bassa</p>
<ul style="list-style-type: none"> <li>- supporti contenenti dati</li> <li>- telefoni</li> </ul>	<p>Si tratterebbe di un furto di copia di dati in quanto non esistono supporti contenenti dati in originale e in singola copia. Possibile trattamento illecito dei dati sottratti.</p> <p>I telefoni non contengono dati memorizzati in locale (i dati delle ultime telefonate ricevute od effettuate sono volatili, spegnendo gli apparecchi per sottrarli i dati si perdono) però c'è il concreto pericolo che l'apparecchio possa essere utilizzato anche al di fuori della rete camerale come se fosse una numerazione camerale. Si rende necessario quindi ricevere prontamente la segnalazione di un'eventuale sottrazione di un apparecchio al fine di disabilitarne, presso il centralino, l'accreditamento dell'apparecchio e le funzionalità.</p>	<p>Grave</p>	<p>Bassa</p>
Danni			
<ul style="list-style-type: none"> <li>- Incendio</li> </ul>	<p>Interruzione del servizio fino al ripristino delle attrezzature danneggiate (se server). I dati sono salvaguardati dalle copie di sicurezza e possono essere ripristinati.</p>	<p>Molto grave</p>	<p>Molto bassa</p>
<ul style="list-style-type: none"> <li>- Interruzione energia elettrica</li> </ul>	<p>Interruzione del servizio fino al ripristino dell'energia elettrica. Non è attualmente previsto un approvvigionamento autonomo o di emergenza. E' previsto un sistema a batterie tampone <b>per i soli server e parte degli apparati attivi</b> di rete per consentire i tempi tecnici di salvaguardia dei dati ed eventualmente protezione da assenza della tensione di breve durata (max. 15/20 minuti)</p> <p>In caso di mancanza di alimentazione anche i telefoni VoIP non saranno funzionanti pertanto si è potenziato l'alimentazione di tutti gli apparati attivi di rete che a loro volta via cavo ethernet forniscono l'alimentazione ai telefoni.</p>	<p>Molto grave</p>	<p>Bassa</p>

	L'autonomia di alimentazione degli apparati telefonici è quindi garantita per 15/20 minuti dalla mancanza di corrente, tempo ritenuto sufficiente per allertare i manutentori per l'eventuale riparazione del guasto		
- Eventi calamitosi naturali ed umani	Interruzione del servizio fino al ripristino delle attrezzature. I dati sono salvaguardati dalle copie di sicurezza. Le copie di sicurezza sono conservate nella stessa località geografica dei server: in caso di calamità particolarmente gravi potrebbero rimanere danneggiate anch'esse	Molto grave	Molto bassa
<b>Rischi logici</b>			
Accessi non autorizzati	Possibili manomissioni alle banche dati, nonché effettuazione di trattamenti non autorizzati. E' un evento molto grave in quanto i danni eventualmente prodotti possono essere non evidenti.	Molto grave	Molto bassa
Virus	Possibili interruzioni della fruizione dei servizi telematici, blocco temporaneo dei sistemi informatici, è però poco rilevante sotto l'aspetto dell'eventuale danneggiamento dei dati. E' un rischio abbastanza alto per la frequenza dei tentativi di attacchi virali registrati ai sistemi. Il sistema di protezione installato è molto aggiornato (aggiornamenti giornalieri o con frequenza superiore). Essendo un attacco con frequenza molto alta, richiede risorse e costante monitoraggio.	Grave	Media
Spyware, malware e worm	Possibili interruzioni della fruizione dei servizi telematici, blocco temporaneo dei sistemi informatici. Possibili manomissioni alle banche dati, nonché effettuazione di trattamenti non autorizzati. E' un evento molto grave in quanto i danni eventualmente prodotti possono essere non evidenti.	Molto grave	Alta
<b>Attacchi ai sistemi informatici</b>			
- Interni	Possibili manomissioni alle banche dati, nonché effettuazione di trattamenti non autorizzati. E' un evento molto grave in quanto i danni eventualmente prodotti possono essere non evidenti.	Molto grave	Molto bassa
- Esterni	Possibili manomissioni alle banche dati, nonché effettuazione di trattamenti non autorizzati. E' un evento molto grave in quanto i danni eventualmente prodotti possono essere non evidenti.	Molto grave	Molto bassa
Vulnerabilità di sistema	Possibili interruzioni della fruizione dei servizi telematici, blocco temporaneo dei sistemi informatici, è abbastanza rilevante sotto l'aspetto dell'eventuale danneggiamento e trattamento non autorizzato dei dati. E' un rischio alto per la frequenza con cui sono segnalate e scoperte falle di sicurezza nei sistemi operativi. Le falle possono essere sfruttate per tutti gli altri tipi di rischi logici,	Molto grave	Media

	<p>vanificando talvolta anche le protezioni messe in atto. Necessita pertanto una costante attenzione ed aggiornamento dei sistemi.</p> <p>Per quanto riguarda i telefoni eventuali vulnerabilità di sistema possono comportare l'interruzione temporanea del servizio ed eventuali malfunzionamenti od indisponibilità di funzioni; il problema è grave soprattutto per la difficoltà di individuare le cause dei problemi e le conseguenti soluzioni derivante dalla complessità del sistema stesso e dai molteplici attori interessati</p>		
--	---	--	--

## Attività e strutture realizzate per la prevenzione dei rischi

Per la prevenzione ed il contrasto dei rischi individuati, sono state poste in atto le seguenti misure di sicurezza:

### Rischi fisici:

- Evento furto o sottrazione:
  - o I locali dove sono ubicate le banche dati sono chiusi e presidiati;
  - o le singole stazioni di lavoro assegnate ad ogni singolo dipendente/addetto al trattamento, sono presidiate, non contengono dati, e consentono il trattamento dei dati, solo se fisicamente connesse alla rete camerale, previa identificazione a mezzo user-id e password.
  - o I telefoni camerali non hanno memoria locale permanente ed è stato organizzato un monitoraggio dei sistemi che segnala l'eventuale scollegamento o malfunzionamento di un apparato telefonico.
  - o La funzionalità degli apparati telefonici sono eventualmente proteggibili e bloccabili con un codice numerico: tale funzionalità consente comunque l'utilizzo delle chiamate ai numeri di emergenza (112, 113, etc.)
  
- Evento danni:
  - o E' stato predisposto un piano di sicurezza e di emergenza contro gli incendi, con la relativa formazione del personale preposto alla gestione di questo tipo di emergenza e sono stati dotati i locali che contengono i dati di opportuni strumenti antincendio a funzionamento manuale;
  - o Contro la mancanza di energia elettrica od eventuali sovratensioni, fulmini etc. è stato predisposto un impianto di terra e un impianto di sezionamento contro le sovratensioni; inoltre le macchine server sono state dotate di batteria tampone della durata di circa 15 minuti ed opportuno software di controllo che provvede al salvataggio dei dati ed allo spegnimento delle macchine per interruzioni di durata superiore.
  - o Contro gli eventi calamitosi sono state predisposte opportune politiche di salvataggio dei dati e delle configurazioni dei server realizzati con apposite librerie a nastro (DLT) e tramite dischi di rete ed è stata implementata una struttura di disaster recovery, che consente il recupero dei dati precedentemente salvati ed la loro messa in pristino in tempi relativamente brevi. Per realizzare ciò si è provveduto a scindere il connubio hardware/Fileserver mediante strumenti di virtualizzazione XenServer Citrix. Tale tecnologia consente un rapido ripristino dei sistemi indipendentemente dall'hardware utilizzato, riducendo così ulteriormente i tempi di un eventuale ripristino.

### Rischi logici:

- Evento accessi non autorizzati:
  - o È stato implementato un sistema di autorizzazione/riconoscimento all'accesso della rete camerale che non consente l'utilizzo della stessa senza le opportune preventive autorizzazioni. I permessi attribuiti ad ogni Utente vengono riconosciuti dal sistema mediante la presentazione di User-id e relativa password; si sta procedendo all'implementazione di un sistema di riconoscimento mediante chiavi digitali e strumenti di certificato digitale e firma elettronica con Smart Card. Il rilascio di tali strumenti di autorizzazione/riconoscimento e la loro revisione sono regolati da quanto previsto nel documento programmatico della sicurezza della Camera di Commercio di Treviso;

- Evento attacchi virali:
  - o Contro tale evenienza sono stati attivati idonei strumenti antivirus aggiornati automaticamente on-line con cadenza giornaliera, e se necessario con maggior frequenza, a mezzo di due strutture di distribuzione parallele una realizzata e gestita da InfoCamere ed una dalla Camera stessa. Il sistema di protezione antivirus è attivato su tutte le stazioni camerali e su tutti i server.
  
- Evento attacchi Spyware, malware e worm:
  - o Contro tale tipo di attacco informatico sono state implementate delle regole di comportamento che minimizzino le possibilità di attacco, nonché sono stati attivati alcuni strumenti antispymware efficaci, seppure con funzionalità di base; E' stata implementata dalla Camera, mediante il proprio prodotto antivirus una soluzione maggiormente automatizzata ed aggiornata.
  - o E' stato predisposto un articolato sistema antispamming composto anch'esso da varie componenti gestite sia da InfoCamere, sui propri sistemi che dalla Camera sul proprio server di posta. Il sistema consente una significativa riduzione degli attacchi di tipo "Phishing" e nella componente della Camera una capacità di reazione più puntuale a questo tipo di campagne. Gli utenti sono ripetutamente informati dei pericoli insiti in questa tipologia di richieste che si basa molto su una attività volontaria, ancorché inconsapevole, del destinatario.
  
- Evento attacchi esterni ed interni ai sistemi informatici:
  - o Come già accennato i collegamenti con l'esterno della rete camerale di Treviso sono effettuati solo ed unicamente a mezzo InfoCamere che pertanto fornisce con opportune strutture e strumenti le necessarie protezioni contro gli attacchi esterni;
  - o Contro gli attacchi provenienti dall'interno sono state attivate le protezioni fisiche degli apparati e dei server di rete, nonché le protezioni logiche all'accesso della rete; inoltre nel documento programmatico della sicurezza con opportuno ordine di servizio e comunicazioni sono state prescritte le norme di comportamento che gli addetti al trattamento dovranno rispettare per garantire la sicurezza (conservazione e segretezza della password, chiudere o bloccare le sessioni di lavoro in caso di assenza dalla stazione, sostituzione della password con cadenza minima di 3/6 mesi e caratteristiche minime della stessa). Tutte le operazioni che possono essere automatizzate dal sistema informatico (scadenza, caratteristiche minime, etc.) sono state attivate.
  - o Vengono svolte periodiche attività formative e di sensibilizzazione a tutto il personale.
  
- Vulnerabilità dei sistemi:
  - o I sistemi informatici non sono perfetti e presentano degli errori che, una volta individuati e scoperti, possono essere sfruttati per aggirare i sistemi di protezione. È necessario pertanto provvedere periodicamente all'analisi dei sistemi installati per la verifica ed individuazione delle vulnerabilità note al fine di consentirne la correzione mediante le opportune attività da individuarsi di volta in volta (applicazione di apposite patch correttive già rilasciate, disabilitazione di servizi pericolosi non necessari, opportune configurazioni dei sistemi).

Il Decreto Legislativo 169/2003 infatti impone, come requisito minimo di sicurezza, l'aggiornamento dei sistemi informatici al fine di eliminare le vulnerabilità note.

A tale scopo sono stati attivati i seguenti servizi: contratto con InfoCamere per l'effettuazione di periodiche analisi dei sistemi informatici camerali con la creazione di rapporti che identificano le vulnerabilità dei sistemi installati ed indicano le possibili soluzioni disponibili.

Sistema di distribuzione delle patch correttive centralizzato ed automatizzato che consente di effettuare l'attività di allineamento di tutte le stazioni operative in uso in

maniera automatizzata all'accensione della macchina, e senza dover operare sulle singole stazioni.

Sistema di monitoraggio automatico attivo 24 ore su 24 di tutti gli eventi critici delle macchine server, con sistema di alerting automatico via posta elettronica agli amministratori dei sistemi ed ai manutentori autorizzati.

Treviso, 28 febbraio 2012

L'Amministratore dei sistemi  
(Angelo Mesina)