Adeguamento alle misure minime di sicurezza

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA DEI DATI

VERSIONE 7.0 ADOTTATA CON DELIBERAZIONE DI GIUNTA CAMERALE N. 20 DEL 22.03.2010

INDICE DEGLI ARGOMENTI

ALLEGATI

PREMESSA

Il presente documento viene redatto secondo quanto prescritto dall'art. 34, comma1, lett.g) e dal Disciplinare Tecnico contenuto nell'Allegato B del Decreto legislativo 30 giugno 2003, n. 196 "*Codice in materia di protezione dei dati personali*" (di seguito denominato Codice o Codice della Privacy).
In particolare, la regola n. 19 del Disciplinare Tecnico richiede ai titolari di trattamento di dati sensibili o giudiziari, mediante strumenti elettronici, di predisporre ed aggiornare, entro il 31 marzo di ogni anno, un Documento Programmatico sulla Sicurezza dei dati (di seguito DPS) che deve contenere idonee informazioni inerenti:

- l'elenco dei trattamenti di dati personali;
- la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;
- l'analisi dei rischi che incombono sui dati;
- le misure di sicurezza adottate o 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;
- la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento degli stessi o degli strumenti elettronici;
- 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 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.

Per giungere ad una efficace e quanto più esaustiva compilazione del presente documento, è stata avviata un'analisi generale dei trattamenti di dati personali effettuati dalla Camera di Commercio Industria Artigianato Agricoltura di Lucca (di seguito C.C.I.A.A. di Lucca): in particolare, sono state censite le banche dati, le misure di sicurezza già poste in essere a tutela dei singoli trattamenti, individuando la loro corrispondenza con quanto previsto dal Disciplinare Tecnico.

Sulla base dei risultati dell'analisi effettuata è stato, quindi, redatto il presente documento. In particolare, vengono utilizzate alcune tabelle, identificate con la stessa numerazione di cui all'elenco dell'art. 19 dell'Allegato B.

Il documento è suddiviso nelle seguenti sezioni:

- **Elenco dei trattamenti di dati personali e delle banche dati**: in cui vengono descritti, in forma tabellare, i trattamenti di dati personali (comuni, sensibili e/o giudiziari) effettuati dalla C.C.I.A.A. di Lucca, nell'ambito di macrocategorie, nonché le banche dati, cartacee ed informatiche, presenti e/o utilizzate presso la stessa.
- **Compiti e responsabilità**: in cui viene illustrato il modello organizzativo della C.C.I.A.A. di Lucca e le relative responsabilità, nonché i trattamenti operati dalle singole strutture ed i compiti delle stesse.
- **Analisi della struttura fisica e dell'infrastruttura informatica**.
- **Analisi dei rischi**: in cui vengono individuati e descritti i principali eventi (minacce ed attacchi) potenzialmente dannosi per la sicurezza dei dati personali trattati dalla C.C.I.A.A. di Lucca

- **Protezione fisica**: in cui vengono definiti i criteri di sicurezza fisica per la protezione dei locali.
- **Protezione logica**: in cui vengono definiti i criteri e le procedure per assicurare l'integrità e la disponibilità dei dati.
- **Formazione degli incaricati del trattamento**: in cui viene descritto il piano di formazione idoneo a rendere edotti gli incaricati del trattamento dei rischi individuati e dei modi per prevenire danni.
- **Verifiche e aggiornamento del DPS**: in cui vengono definite le linee guida per l'elaborazione di un piano di svolgimento delle attività di verifica ed aggiornamento del DPS.

1. ELENCO DEI TRATTAMENTI DI DATI PERSONALI E DELLE BANCHE DATI

In questa sezione sono individuati i trattamenti effettuati dal titolare, direttamente o attraverso soggetti esterni, con l'indicazione della natura dei dati, della struttura, interna od esterna, operativamente preposta o concorrente al loro trattamento, nonché degli strumenti impiegati.

A tale scopo, si riportano due tabelle.

Nella prima tabella (denominata *tab. 19.1 Trattamenti di dati* – allegato a), per ciascun macrotrattamento, individuato nella prima colonna con un identificativo numerico per agevolarne il successivo richiamo e descritto nella seconda, vengono indicate le tipologie dei trattamenti effettuati, anch'essi identificati numericamente (colonna 3) e di seguito descritti (colonna 4). Nelle colonne successive sono riportate le seguenti informazioni:

Dati: vengono descritti sinteticamente i dati trattati e le categorie di persone cui essi si riferiscono.

Natura dei dati trattati: viene specificato se si tratta di dati personali cosiddetti comuni[1], sensibili[2] e/o giudiziari[3].

Struttura di riferimento: viene indicata la struttura (ufficio, funzione, ecc.) all'interno della quale viene effettuato il trattamento.

Altre strutture che concorrono al trattamento: nel caso in cui un trattamento, per essere completato, comporti l'attività di diverse strutture, vengono indicate, oltre quella che cura primariamente l'attività, le altre principali strutture che concorrono al trattamento anche dall'esterno.

Nella successiva tabella (denominata *tab. 19.1 bis Banche dati* – allegato b) sono indicati ulteriori elementi descrittivi degli strumenti impiegati per i trattamenti, attraverso le seguenti informazioni:

Identificativo del trattamento: numero che consente il collegamento con la precedente tabella.

Banca dati: viene indicata la banca dati presente e/o utilizzata presso l'Ente.

Natura e descrizione sintetica della banca dati: in particolare, viene indicata la natura della banca dati – cartaceo e/o informatica - , nonché il tipo di dati in essa contenuti.

[1] Per *dato personale comune* si intende "qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale" (art. 4 comma 1 lettera b) Codice della Privacy).

[2] Per *dati sensibili* si intendono "i dati personali idonei a rivelare l'origini 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" (art. 4 comma 1 lettera d) Codice della Privacy).

[3] Per *dati giudiziari* si intendono "i dati personali idonei rivelare provvedimenti di cui all'art. 3, comma 1, lettere da a) a o) e da r) a u), del DPR 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" (art. 4 comma 1 lettera e) Codice della Privacy).

Ubicazione archivio cartaceo: viene indicato la struttura di riferimento, con l'indicazione della sua ubicazione all'interno della sede camerale.

Luogo logico: nel caso di dati contenuti in banche dati informatiche, viene indicato il supporto di memorizzazione utilizzato (server camerale o esterno, disco fisso della singola postazione, floppt disk, CD-Rom).

Luogo fisico: viene indicato il luogo in cui risiedono fisicamente i dati ovvero dove si trovano (in quale sede, centrale o periferica, o presso quale soggetto esterno) gli elaboratori sui cui dischi sono memorizzati i dati, i luoghi di conservazione dei supporti magnetici utilizzati per le copie di sicurezza (nastri, CD, ecc.) ed ogni altro supporto rimovibile.

Tipologia di dispositivi di accesso: elenco e descrizione sintetica degli strumenti utilizzati dagli incaricati per effettuare il trattamento: personal computer (PC), terminale non intelligente, palmare, telefonino, ecc.

Tipologia di interconnessione: descrizione sintetica e qualitativa della rete che collega i dispositivi d'accesso ai dati utilizzati dagli incaricati: rete locale, geografica, Internet, ecc.

2. COMPITI E RESPONSABILITÀ

Titolare del trattamento dei dati personali – ai sensi dell'art. 28 del Codice della Privacy - è la Camera di Commercio Industria Artigianato Agricoltura di Lucca con sede in Lucca – Corte della Campana, 10 – CAP 55100.

Tutti i trattamenti effettuati all'interno della C.C.I.A.A. di Lucca sono improntati al principio di necessità, di liceità e di correttezza e sono finalizzati in via esclusiva allo svolgimento delle attività istituzionali che la legge n. 580 del 29 dicembre 1993, così come successivamente attuata, integrata e modificata, nonché la precedente normativa dalla stessa non abrogata, attribuisce alle Camere di Commercio.

L'ente camerale opera attraverso il proprio organo esecutivo, la Giunta, le cui competenze e funzioni sono individuate nelle disposizioni di legge e statutarie vigenti. La rappresentanza legale spetta al Presidente *pro tempore*.

Alla Camera di Commercio, in qualità di titolare del trattamento, competono le decisioni in ordine alle finalità ed alle modalità del trattamento[4] dei dati personali ed agli strumenti utilizzati, ivi compresi i profili attinenti la sicurezza.

La Camera potrà inoltre rivestire la qualità di responsabile di trattamenti affidati da altri soggetti pubblici o da associazioni/partecipate camerali; in tali casi la Giunta ha delegato ai responsabili interni competenti, l'individuazione degli incaricati e l'indicazione dei trattamenti consentiti dal soggetto terzo, titolare dei trattamenti stessi.

L'**assetto organizzativo** della C.C.I.A.A. di Lucca, così come definito dalla Giunta camerale con deliberazione n. 44 del 21 giugno 2006, con decorrenza 1° luglio 2006, prevede n. 4 aree dirigenziali, articolate in Servizi ed Uffici e di seguito specificate: Area del Segretario Generale, Area Anagrafico Certificativa e Regolazione del Mercato, Area Amministrazione e Personale, Area Promozione e Sviluppo per le Imprese.

In conformità a tale assetto organizzativo, con le determinazioni del Segretario Generale n. 623/2005 e n. 97/2007 e con delibera di Giunta n. 23/2009 sono stati nominati quali **responsabili interni del trattamento dei dati personali** le persone che rivestono la qualifica di dirigente, specificandone analiticamente i compiti ed impartendo loro adeguate istruzioni. Con gli stessi atti sono stati altresì individuati gli incaricati nei dipendenti presenti nella dotazione della struttura organica degli uffici o comunque ad essa assegnati, salvo diversa indicazione scritta di ciascun responsabile direttamente ai propri incaricati, individuandone l'ambito di trattamento consentito nei trattamenti individuati per ciascun ufficio nell'allegato C.
Il Segretario Generale ha altresì provveduto a fare idonee comunicazioni di servizio.

Agli effetti della normativa in materia di privacy, sono equiparati ai lavoratori dipendenti a tempo indeterminato tutti coloro che - a vario titolo e, dunque, a prescindere dal rapporto giuridico sottostante - collaborano con la C.C.I.A.A. di Lucca nello svolgimento delle attività istituzionali (ad esempio, lavoratori dipendenti a tempo determinato, lavoratori temporanei, borsisti, stagisti, collaboratori esterni a progetto o occasionali), impegnandosi formalmente al rispetto delle disposizioni dettate dalla normativa vigente in materia e dall'atto che disciplina il rapporto di collaborazione.

[4] Per *trattamento* si intende "qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernente 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" (art. 4 comma 1 lettera a) Codice della privacy).

I responsabili e gli incaricati del trattamento, nell'effettuare le operazioni di trattamento di competenza, dovranno attenersi oltre che alle disposizioni vigenti in materia, alle istruzioni loro impartite e rispettare le misure di sicurezza per la protezione dei dati personali individuate nel presente documento.

In particolare gli incaricati:
- svolgono le attività previste secondo gli indirizzi del responsabile;
- non modificano i trattamenti esistenti o ne introducono di nuovi senza esplicita autorizzazione del responsabile;
- rispettano e fanno rispettare nell'autorizzare, per quanto di propria competenza, l'accesso di soggetti esterni ai locali camerali, e eventualmente alla documentazione amministrativa in base al regolamento camerale e alla normativa vigente in materia di accesso, la normativa vigente in materia di privacy e le disposizioni contenute nel presente documento;
- informano il responsabile in caso di incidente di sicurezza che coinvolga i dati personali;
- si attengono ai criteri di cui al capitolo 6 nel definire le proprie password di accesso alle varie applicazioni informatiche;
- utilizzano i dati in modo lecito e secondo correttezza;
- raccolgono e registrano dati personali esclusivamente per scopi inerenti le funzioni assegnate nell'ambito del servizio o dell'ufficio, non eccedendo il limite delle finalità per cui sono raccolti e trattati;
- assicurano la massima riservatezza dei dati trattati e custoditi;
- accedono ai soli dati personali la cui conoscenza sia necessaria per adempiere ai compiti assegnati;
- conservano atti e documenti in trattazione adottando la massima riservatezza per il tempo strettamente necessario all'adempimento delle operazioni affidate;

Con delibera n. 20 del 22 marzo 2010 sono stati nominati gli amministratori di sistema specificando le tipologie di trattamenti effettuati all'identificativo 30 della tabella 19.1.

La tabella (denominata *tab. 19.2 Compiti e responsabilità* – allegato c) riporta le seguenti informazioni:

Struttura: indicazione della struttura camerale in cui si realizza il trattamento, secondo quanto già riportato nella tabella 19.1.

Trattamenti effettuati dalla struttura: vengono specificati i trattamenti di competenza di ciascuna struttura, utilizzando quanto già descritto nella tabella 19.1.

Compiti e responsabilità della struttura: vengono descritti sinteticamente i compiti e le responsabilità della struttura rispetto ai trattamenti di competenza.

3. ANALISI STRUTTURA FISICA E ANALISI INFRASTRUTTURA INFORMATICA

3.1 ANALISI STRUTTURA FISICA

La Camera di Commercio I.A.A. di Lucca ha sede principale a Lucca in un immobile sito in Corte della Campana n. 10.
Alla sede principale di Lucca si accede da Corte della Campana, nonché da piazza della Cervia. Il primo accesso è utilizzabile dagli utenti negli orari di apertura (dal lunedì al venerdì dalle ore 09:00 alle ore 13:00 ed il lunedì ed il mercoledì anche dalle ore 15:00 alle ore 16:00). Il secondo accesso è esclusivamente riservato ai dipendenti (tramite badge) ed ai soggetti specificatamente autorizzati (personale addetto alle pulizie[5], imprese esecutrici di lavori, personale di Lucca Promos e Italdom, etc.).
Per favorire l'utenza, in relazione a taluni servizi (Registro imprese, Albo imprese artigiane, REC Albi e Ruoli, Commercio estero e Firma digitale) e con orari di apertura diversificati, sono presenti sul territorio provinciale alcune sedi distaccate: a Viareggio in via Leonida Repaci (quartiere Marco Polo), a Castelnuovo di Garfagnana (c/o locali della Comunità Montana), a Fornaci di Barga.

3.2 ANALISI INFRASTRUTTURA INFORMATICA

Il sistema informatico della C.C.I.A.A. di Lucca è basato su un insieme di reti locali, una per ciascuna sede fisica, tra loro collegate tramite linea HDSL-ISDN.
La sede principale di Lucca, sita in Corte della Campana n. 10, è inoltre collegata alla sede operativa di Infocamere ScpA a Padova in Corso Stati Uniti n. 14, tramite una connessione CDN e dalla struttura di Infocamere è possibile l'interconnessione con la rete pubblica Internet.
Tutte le postazioni di lavoro presso gli uffici camerali e gli uffici di Lucca Promos, Italdom e Lucca Intech sono abilitate all'accesso su Internet e all'utilizzo della posta elettronica.
La connessione ad Internet avviene utilizzando la rete privata di Infocamere e il nodo di interconnessione alla rete pubblica gestito dalla stessa società: questo, insieme all'adozione di un adeguato firewall e alla procedura organizzativa che vieta l'utilizzo di modem sui pc camerali, garantisce un livello adeguato di protezione della rete interna.

La C.C.I.A.A. di Lucca dispone dei seguenti server aziendali, ubicati fisicamente presso il Centro Elaborazione Dati al terzo piano della sede principale:

- n. 2 server Windows 2000 di cui il principale contiene gli archivi comuni dell'Ente, mentre il secondario provvede allo scambio di informazioni e replica l'Active Directory (AD) in simultanea con il principale.
  In questo modo, in caso di disaster recovery, il recupero di informazioni di fondamentale importanza relative all'AD è totale.
- n. 1 server virtuale VMWare per la gestione di applicazioni relative alle direttive privacy e di altre necessarie applicazioni

[5] Il servizio di pulizia del locali camerali è svolto da personale (n. 3 unità) della Co.g.e.o. dal lunedì al venerdì, con i seguenti orari: lunedì e mercoledì dalle ore 17.30 alle ore 20.30, nei restanti giorni dalle 14.30 alle 17.30. La cooperativa effettua inoltre interventi straordinari di pulizia su richiesta.

- n. 1 server Linux per la gestione della Intranet della C.C.I.A.A. di Lucca.

Oltre ai server sopra indicati presso l'ufficio personale è ubicato n. 1 pc server per applicativo di rilevamento telefonate effettuate dal personale camerale.

Le rimanenti applicazioni sono ad oggi installate sui singoli pc degli incaricati e gli archivi sono condivisi a livello di aree/servizi/uffici attraverso l'accentramento sui server dedicati per facilitare le operazioni di Back-Up.

La C.C.I.A.A. di Lucca dispone di un proprio sito web (www.lu.camcom.it) e di un sito inerente l'archivio storico in hosting presso la partecipata camerale Lucense ScpA di Lucca.

Il locale contenente le apparecchiature di natura informatica (server, apparati di rete ecc.) e di trasmissione dati (armadio switch/Hub, router) è situato al terzo piano dell'immobile camerale sito in Corte della Campana, 10 – Lucca.

4. ANALISI DEI RISCHI

Le necessità di sicurezza vengono valutate in relazione alle minacce cui è sottoposto il sistema informativo oggetto dell'analisi. La conoscenza di tali minacce è essenziale nell'iter metodologico per l'individuazione e la progettazione delle misure di protezione che possono concretizzarsi in meccanismi di natura logica (uso password, antivirus, ecc.), di natura fisica (meccanismi di antintrusione, controllo di accesso ai locali, ecc.) e soluzioni di natura organizzativa (procedure, normativa interna).

Il processo di analisi si sviluppa, quindi, nei seguenti passi:
- individuazione delle minacce
- identificazione degli attacchi mediante i quali le minacce possono realizzarsi
- individuazione delle possibili correlazioni tra le minacce e gli attacchi

MINACCE

Con il termine *minaccia* si intende la potenziale "causa" di un attacco indesiderato che può produrre un danno al patrimonio informativo. Nella seguente tabella sono riportate una serie di possibili minacce:

Minaccia	Descrizione
Furto	Azioni di appropriazione di informazioni, dispositivi, impianti, supporti magnetici o copie di dati e/o programmi
Dolo	Frodi o inganni finalizzati ad arrecare un danno per ricavarne profitti illeciti da parte sia di personale interno infedele che esterno
Danneggiamento	Eventi che danneggiano il sistema sia fisicamente che logicamente e che comportano la perdita di disponibilità delle informazioni o l'interruzione del servizio
Errori della tecnologia	Errori derivanti da malfunzionamenti hardware o software
Errori operativi	Errori umani nell'operare sul sistema
Guasti dei sistemi	Indisponibilità del sistema a causa di guasti o inefficienza hardware e/o software
Inagibilità dei locali	Condizioni di impraticabilità temporanea o definitiva dei locali

ATTACCHI

Con il termine *attacco* si intende una delle possibili modalità con cui una minaccia può essere perpetrata. Di seguito si elencano gli attacchi più rilevanti con cui le minacce, elencate al paragrafo precedente, possono essere attuate.

Attacchi	Descrizione
Accesso non autorizzato ai locali e/o agli archivi cartacei	Introduzione di persone non autorizzate nei locali dove ha luogo il trattamento o sono custoditi gli archivi
Evento distruttivo di origine naturale	Eventi naturali in grado di interrompere la funzionalità di un sistema
Azione distruttiva di natura fisica intenzionale	Azioni distruttive volontarie capaci di compromettere l'integrità fisica di un sistema
Azione distruttiva di natura fisica non intenzionale	Azioni distruttive involontarie capaci di compromettere l'integrità fisica di un sistema
Furto di apparati informatici	Asportazione di alcune componenti del sistema
Furto di supporti informatici e documenti cartacei	Asportazione di nastri, floppy disk, CD Rom, tabulati, modulistica
Accesso non autorizzato alle informazioni su archivi informatici	Accesso, da parte di persone non autorizzate, a dati presenti su archivi informatici, con possibilità di copia, modifica o cancellazione
Impersonamento in altro soggetto	Accesso ai dati con credenziali di altra persona
Intercettazione delle informazioni dai terminali	Intercettazione delle informazioni messa in atto senza violare il meccanismo di controllo accesso (es. utilizzo di una sessione lasciata incustodita)
Accesso non autorizzato a documenti cartacei	Lettura, copia o sostituzione non autorizzata di documenti, tabulati, modulistica contenenti informazioni e conservati in archivi
Accesso non autorizzato di messaggi in rete	Estrazione, manomissione o cancellazione non autorizzata delle informazioni contenute in messaggi in rete
Modifica non autorizzata dell'instradamento	Alterazione non autorizzata delle informazioni che guidano l'instradamento dei messaggi
Modifica non autorizzata della configurazione software	Modifica degli eseguibili del software o inserimento di software non autorizzato
Abuso di privilegi	Utilizzo dei privilegi ricevuti per scopo diverso da quello

Attacchi	Descrizione
	assegnato al proprio ruolo
Guasto hardware	Cattivo funzionamento di apparati che comporta la perdita di affidabilità dei sistemi dovuto, ad esempio, a difetti di fabbricazione, usura
Errore nel software	Cattivo funzionamento del software dovuto, ad esempio, a difetti propri del software o a sua manomissione
Interruzione dei servizi	Interruzione dei servizi di energia elettrica, condizionamento, etc.

CORRELAZIONE TRA MINACCE, ATTACCHI E GRAVITÀ

La tabella di correlazione riportata di seguito indica, per ogni minaccia, gli attacchi con cui questa può essere perpetrata.
Va evidenziato che, data la natura dei dati trattati e le caratteristiche del trattamento, si è stimata una probabilità bassa del verificarsi degli attacchi, con conseguenze trascurabili sull'integrità, sulla riservatezza e sulla disponibilità dei dati.

ATTACCHI	PERSONALE INTERNO	PERSONALE ESTERNO	HACKER	GUASTI E MALFUNZIONAMENTI	INCIDENTI E CALAMITÀ
Accesso non autorizzato ai locali e/o agli archivi cartacei	**X**	**X**			
Evento distruttivo di origine naturale					**X**
Azione distruttiva di natura fisica intenzionale	**X**	**X**			
Azione distruttiva di natura fisica non intenzionale	**X**				**X**
Furto di apparati informatici	**X**	**X**			
Furto di supporti informatici e documenti cartacei	**X**	**X**			
Accesso non autorizzato alle informazioni su archivi informatici	**X**	**X**	**X**	**X**	
Impersonamento in altro soggetto	**X**	**X**	**X**		
Intercettazione delle informazioni dai terminali	**X**	**X**	**X**		

Accesso non autorizzato a documenti cartacei	**X**	**X**			
Accesso non autorizzato di messaggi in rete	**X**	**X**	**X**	**X**	
Modifica non autorizzata dell'instradamento			**X**		
Modifica non autorizzata della configurazione software	**X**	**X**	**X**	**X**	
Abuso di privilegi	**X**	**X**			
Guasto hardware				**X**	
Errore nel software			**X**	**X**	
Interruzione servizi energia elettrica, condizionamento, etc.				**X**	**X**

5. PROTEZIONE FISICA

Presso la C.C.I.A.A. di Lucca sono presenti i seguenti sistemi di protezione di tipo fisico, validi anche per i locali in comodato a Lucca Promos, Italdom e Lucca Intech:

CONTROLLO ACCESSI FISICI	Durante l'orario di lavoro, presso la sede camerale principale di Lucca, è presente un servizio di portineria e controllo accessi: una postazione di reception, ubicata al piano terra, ha il compito di identificare i visitatori occasionali o temporanei (es. collaboratori che prestano la loro opera all'interno della struttura) e di controllarne ingresso ed uscita. Relativamente al personale camerale e di Lucca Promos, al personale addetto alla pulizia e alle manutenzioni, la registrazione dell'ora d'ingresso e di uscita avviene, invece, tramite badge.
ANTINTRUSIONE E VIGILANZA	L'accesso all'immobile camerale sito in Corte della Campana è parzialmente protetto da sistemi di antintrusione. Un servizio di vigilanza è, inoltre, svolto dall'istituto di polizia privata 'Fidelitas s.p.a.' di Mugnano (Lucca) (apertura/chiusura giornaliera delle porte di ingresso della sede camerale principale di Lucca, collegamento radio con la sede stessa, passaggio notturno giornaliero con bigliettazione presso gli uffici distaccati di Viareggio).
IMPIANTI AUSILIARI	Nei locali degli immobili camerali sono presenti impianti di continuità elettrica (UPS) e di climatizzazione. Presso i magazzini di Lucca e Carraia (Via Tazio Nuvolari) è attivo un sistema antincendio collegato all'istituto di polizia privata "Fidelitas s.p.a.", già operativo presso il magazzino di Piazza della Cervia.
LIMITAZIONE ACCESSO AI LOCALI TECNICI	L'accesso, onde evitare accessi indesiderati, è consentito solo al personale autorizzato e le chiavi sono custodite presso l'Ufficio Provveditorato.
VIDEOSORVEGLIANZA	L'immobile è protetto tramite 7 videocamere posizionate rispettivamente sul lato interno Piazza della Cervia direzionata verso la porta di ingresso, sul lato esterno Piazza della Cervia direzionata su zona porta ingresso, sul lato esterno Piazza della Cervia direzionata su zona porta antipanico, sul lato interno Corte Campana n. 2 direzionate verso la porta ingresso (bussola), sul lato esterno Corte Campana n. 2 direzionate su zona porta ingresso.

La Camera ha nominato quale responsabile della sicurezza ing. Giovanni Dell'Osso.

I fascicoli delle imprese e degli iscritti in albi, ruoli o registri tenuti dalla Camera di Commercio, i fascicoli del personale, anche relativo al personale di Lucca Promos, i documenti inerenti procedure di concorso, le pratiche relative agli uffici ragioneria, Provveditorato e Diritto annuale, nonché ogni altro archivio cartaceo contenente dati sensibili e/o giudiziari, sono custoditi in locali o in contenitori muniti di serratura, le cui chiavi sono custodite presso i competenti uffici, e sono sotto il controllo e la custodia del personale incaricato del trattamento dei dati stessi.

L'eventuale accesso di soggetti esterni alla documentazione cartacea dovrà essere autorizzato dagli incaricati del trattamento dei dati, che dovranno impartire specifiche disposizioni volte a garantire il rispetto della normativa vigente in materia di privacy e vigilare sul rispetto delle stesse.

I dati idonei a rilevare lo stato di salute vengano conservati separatamente da ogni altro dato trattato per finalità che non richiedono il loro utilizzo. Laddove non sia possibile procedere ad una conservazione separata di tali dati, questi devono essere conservati in sezioni o sottofascicoli, da conservare chiusi o con modalità tali da ridurre la possibilità di una indistinta consultazione nel corso delle ordinarie attività amministrative.

I supporti di memorizzazione (floppy disk, CD Rom, altro) devono essere custoditi dagli incaricati con la necessaria diligenza, al fine di evitare accessi non autorizzati e trattamenti non consentiti. Nel caso in cui non sia più necessario conservare tali supporti per gli scopi per cui erano stati raccolti e trattati, devono essere distrutti o resi inutilizzabili.

6. PROTEZIONE LOGICA

Di seguito vengono riportate le misure di sicurezza già adottate e da adottare in caso di trattamento di dati personali con strumenti elettronici, in conformità a quanto previsto dall'allegato B (Disciplinare tecnico in materia di misure minime di sicurezza) del Codice della Privacy. Quanto di seguito descritto vale anche per Lucca Promos, Italdom e Lucca Intech secondo quanto specificato nel punto 3.

IDENTIFICAZIONE E AUTENTICAZIONE

L'utilizzo delle strutture informatiche e l'accesso agli applicativi di InfoCamere e sue partecipate, nonché agli archivi condivi sul server camerale è consentito agli incaricati, nell'esercizio delle proprie mansioni, previo rispetto di una procedura di identificazione e di autenticazione. Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica; le credenziali sono, altresì, disattivate, qualora vengano meno le qualità che consentono all'incaricato l'accesso ai dati personali.

IDENTIFICAZIONE E AUTENTICAZIONE TRAMITE USER-ID

Codice Identificativo (user-id)	Agli incaricati del trattamento di dati personali è attribuito un codice identificativo personale per accedere alla rete intranet aziendale e/o internet.
Parola Chiave (password)	Al codice identificativo è associata una password riservata e personale che viene assegnata inizialmente in via automatica dai sistemi operativi e dalle applicazioni e che l'incaricato, dopo l'installazione ed al primo utilizzo, ha l'obbligo di modificare osservando le seguenti regole : • la password deve essere alfanumerica e cioè contenere almeno un carattere alfabetico ed uno numerico; • deve essere di lunghezza non inferiore a 8 caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, di un numero di caratteri pari al massimo consentito; • non deve contenere riferimenti agevolmente riconducibili all'incaricato (ad esempio, il nome e/o la data di nascita proprio o di familiari);
Parola Chiave (password)	• non deve essere ottenuta anagrammando la precedente o essere comunque simile alle precedenti; • la password deve essere sostituita almeno ogni 6 mesi nel caso vengano trattati dati personali comuni ed almeno ogni 3 mesi in caso di trattamento di dati sensibili e/o giudiziari; • non deve essere riutilizzata da altri incaricati o comunicata ad altri utenti, neanche per un utilizzo temporaneo o in caso di emergenza; • non deve essere trascritta su carta né memorizzata su supporto magnetico o, più in generale, conservata in luogo facilmente accessibile a terzi.

Criteri e Procedure di rilascio di user-id e password	Ogni utente riceve una user-id per gli applicativi che lo richiedono.
Criteri e Procedure di controllo accessi agli archivi informatici	L'accesso agli archivi informatici è controllato da un sistema congruente con l'applicativo/piattaforma utilizzato sulla base delle abilitazioni corrispondenti ai profili di appartenenza.

IDENTIFICAZIONE E AUTENTICAZIONE TRAMITE SMART CARD

Identificativo Univoco dell'Utente (IUT) – Smart Card	Al fine di garantire l'univoca identificazione degli incaricati del trattamento di dati personali, a ciascuno di essi è attribuito un codice identificativo unico e univoco, contenuto nella smart card stessa.
PIN (Personal Identification Number)	Il PIN è un codice personale e segreto, di lunghezza variabile da 5 a 8 caratteri, gestito e conosciuto esclusivamente dall'utente, necessario per accedere alle procedure abilitate all'autenticazione tramite smart card.
Criteri e Procedure di rilascio del codice identificativo	La smart card viene emessa su richiesta del responsabile del procedimento e rilasciata completa del codice pin e del relativo dispositivo di lettura. Tramite tale lettore, che deve essere collegato al pc, avviene l'autenticazione dell'utente.
Criteri e Procedure di controllo accessi agli archivi informatici	L'accesso agli archivi informatici è controllato da un sistema congruente con l'applicativo/piattaforma utilizzato sulla base delle abilitazioni corrispondenti ai profili di appartenenza.

CONTROLLO ACCESSO LOGICO

L'accesso ai dati è regolato attraverso l'attribuzione ad ogni incaricato di uno specifico profilo. I profili-utente sono alla base del controllo degli accessi e vengono precostituiti in base all'area di appartenenza dell'incaricato, dagli addetti alle funzioni informatiche su indicazione del dirigente d'area.

L'accesso alle strutture informatiche è inoltre consentito alle imprese specializzate per la manutenzione dell'hardware e del software incaricate dalla Camera di Commercio, sotto la supervisione degli addetti alle funzioni informatiche.

USO DEL PC

Gli incaricati non devono lasciare incustodito e accessibile lo strumento elettronico durante la sessione di trattamento. Al fine di garantire la protezione dell'accesso delle postazioni di lavoro accese e non utilizzate, si prescrive di attivare l'opzione, offerta dal sistema operativo, di Screen Saver Lock.

Per quanto riguarda la gestione delle banche dati informatiche che risiedono sul disco fisso, ciascun incaricato è tenuto ad effettuare delle copie di salvataggio delle stesse con frequenza almeno settimanale.

ASSENZA DELL'INCARICATO

In caso di prolungata assenza o impedimento dell'incaricato e necessità di intervento per garantire l'operatività e la sicurezza del sistema, la disponibilità dei dati o strumenti elettronici è assicurata dalla presenza di una copia delle credenziali in uso presso l'addetto camerale alle funzioni informatiche (ufficio Provveditorato). Tale addetto ha l'obbligo di custodire le credenziali in modo tale da garantirne la segretezza, nonché di comunicare tempestivamente, in caso di intervento, all'incaricato assente o impedito il tipo di intervento effettuato.

TRACCIAMENTO

Sono presenti meccanismi di registrazione degli accessi alle risorse del sistema rilevanti per gli aspetti di sicurezza.

RIUTILIZZO DEI SUPPORTI

I supporti di memorizzazione potranno essere riutilizzati solo nel caso in cui le informazioni precedentemente memorizzate non siano tecnicamente in alcun modo recuperabili; in caso contrario detti supporti dovranno essere distrutti.

ANTIVIRUS

Per la prevenzione dei rischi derivanti dall'introduzione di programmi contenenti virus, sono state adottate misure di natura tecnica: tra queste, un sistema antivirus con funzionalità automatiche di aggiornamento sia sul server che sulle singole postazioni di lavoro.

7. CRITERI E MODALITA' DI RIPRISTINO DELLA DISPONIBILITA' DEI DATI

I dati presenti sui server camerali, registrati nelle banche dati informatiche ubicate logicamente sui server stessi, vengono salvati con frequenza giornaliera secondo le modalità definite nel contesto dei singoli applicativi installati sui server stessi.
I backup vengono effettuati su libreria che può contenere fino a 7 nastri DLT-LT01, con una capacità per nastro fino a 200 Gb e gestiti da un software professionale Veritas Backup Exec con le seguenti opzioni:

- salvataggio files aperti (ADVANTAGE OPEN FILE OPTION)
- Intelligence Disaster Recovery con la quale si crea l'immagine dei Servers in modo da ridurre i tempi di ripristino della macchina
- Almeno due test all'anno di Disaster Recovery

PIANO BACKUP

	Nastro 1 (200GB)	Nastro 2 (200GB)	Nastro 3 (200GB)	Nastro 4 (200GB)	Nastro 5 (200GB)	Nastro 6 (200GB)	Nastro clean
lunedì	**x**						
martedì		**x**					
mercoledì			**x**				
giovedì				**x**			
venerdì					**x**		
sabato						**x**	
domenica							**c**

x: backup giornaliero totale degli archivi
c: cleaning settimanale

Fino ad esaurimento delle cassette, i successivi backup verranno appesi.
Una volta esaurita la capacità di scrittura (30 volte circa), le cassette verranno sostituite.
Solo la cassetta del backup del sabato non viene soprascritta, ma mantenuta in luogo protetto in modo da avere sempre una copia di backup almeno settimanale.

Le copie di backup sono conservate in un armadio chiuso a chiave, ubicato presso la sala CED, a cui hanno accesso i soli Amministratori di Sistema incaricati di eseguire le operazioni di salvataggio.

8. PIANIFICAZIONE DEGLI INTERVENTI FORMATIVI

In via generale, la C.C.I.A.A. di Lucca proseguirà l'attività di sensibilizzazione nei confronti dei responsabili interni e degli incaricati del trattamento, con particolare riferimento alle modifiche apportate al DPS.

Sarà cura del responsabile, nel caso di nuovi ingressi in servizio, o di introduzione di nuovi e significativi strumenti attraverso cui vengono effettuati i trattamenti e/o modifica sostanziale di quelli già utilizzati, istruire gli addetti in merito alle misure di sicurezza da adottare.

Inoltre, laddove ritenuto opportuno in relazione all'emergere di specifiche necessità operative, eventualmente segnalate dai responsabili, saranno realizzate ulteriori iniziative di formazione avanzata o di aggiornamento, idonee ad assicurare la corretta comprensione ed applicazione della normativa in materia.

9. TRATTAMENTI AFFIDATI ALL'ESTERNO

Nell'ambito dei macrotrattamenti e dei trattamenti individuati nella tabella 19.1, vi sono talune attività, allo svolgimento delle quali concorrono o che sono affidate - o comunque suscettibili di essere affidate - a soggetti esterni (società, enti, consulenti).
Tali soggetti, a seconda dei casi, possono rivestire il ruolo di incaricato esterno, di responsabile esterno o di titolare del relativo trattamento, in via esclusiva o in titolarità con la Camera di Commercio.

In particolare il Sig. *Marcello Petrozziello*, giornalista pubblicista, è stato incaricato dalla Camera di Commercio di svolgere, in concorso con l'ufficio camerale Relazioni esterne, nell'ambito del macrotrattamento 20, delle attività connesse ai trattamenti contraddistinti dall'identificativo 20.1, afferenti esclusivamente dati personali comuni.

Altri soggetti potranno assumere la qualifica di incaricati esterni sulla base di specifici atti di conferimento, convenzioni, etc. In ogni caso, al fine di garantire un adeguato trattamento dei dati, è necessario che il soggetto esterno a cui viene affidato il trattamento rilasci specifiche dichiarazioni o documenti, oppure assuma alcuni impegni anche su base contrattuale, con particolare riferimento, ad esempio, a:

- trattamento di dati ai soli fini dell'espletamento dell'incarico ricevuto;
- adempimento degli obblighi previsti dal Codice per la protezione dei dati personali, con particolare riferimento all'adozione delle misure di sicurezza;
- rispetto delle istruzioni specifiche eventualmente ricevute per il trattamento dei dati personali, soprattutto se di natura sensibile e/o giudiziaria, o integrazione delle procedure già in essere;
- impegno a relazionare periodicamente sulle misure di sicurezza adottate – anche mediante eventuali questionari e liste di controllo - e ad informare immediatamente il titolare del trattamento in caso di situazioni anomale o di emergenze.

La Camera di Commercio di Lucca ha individuato, tra l'altro, quali responsabili esterni:

InfoCert s.p.a., la Società Consortile delle Camere di Commercio per azioni InfoCamere e le società controllate da Infocamere, I.C. Technology, I.C. Service, Infobusiness, EcoCerved, ICOutsourcing, per quanto riguarda i trattamenti effettuati dalle stesse con la gestione di varie banche dati secondo quanto previsto dai patti consortili e/o da specifici accordi contrattuali;

la Società Consortile per Azioni Lucense di Lucca in relazione ai trattamenti effettuati per la gestione del sito e della intranet camerale;

Retecamere s.c.r.l. di Roma, in relazione ai dati personali comuni trattati per la gestione degli indirizzari tramite la piattaforma CRM;

Lucca Promos s.c.r.l. in relazione ai dati trattati nella realizzazione di progetti affidati dalla Camera;

Firenze Tecnologia, azienda speciale della C.C.I.A.A. di Firenze in relazione ai dati trattati per la richiesta e/o attivazione di procedure di conciliazione.

Operano in qualità di titolari del trattamento, tra l'altro, come meglio specificato nelle tabelle allegate:

- la *Regione Toscana* in sede di rinnovo del Consiglio camerale;
- il *Monte dei Paschi di Siena* – filiale di Lucca, per i trattamenti che svolge quale istituto di credito aggiudicatario del servizio di tesoreria della Camera di Commercio;
- l'*Associazione 'Lucchesi nel Mondo'* in relazione ai dati personali comuni trattati nell'ambito della Premiazione dei Lucchesi che si sono distinti all'estero;
- il *Ministero dello Sviluppo Economico* e l'*ISTAT* in relazione al trattamento dei dati personali comuni elaborati per la realizzazione di statistiche o osservatori vari;
- l'*Ufficio Italiano Brevetti e Marchi* (UIBM) in relazione ai dati personali comuni trattati per la registrazione di marchi e brevetti;
- Equitalia s.p.a. in qualità di gestore delle procedure post ruolo a livello nazionale;
- Equitalia Cerit s.p.a. in qualità di concessionario del servizio di riscossione tributi;
- l'*Agenzia per le erogazioni in agricoltura* (AGEA) in relazione ai dati personali comuni trattati per la gestione degli amidi;
- *Comunità Montana, Via Vittorio Emanuele, 9 Castelnuovo Garfagnana,* in relazione ai dati personali comuni, sensibili e giudiziari trattati in sede di rilascio visure e smart card.
- *O*gni altro soggetto indicato nella colonna "altre strutture, anche esterne" della tabella 19.1, per il quale non sia stata specificata la qualifica di responsabile esterno.

10. VERIFICHE ED AGGIORNAMENTO DEL DPS

Le misure di cui al presente documento saranno oggetto di verifiche periodiche – almeno annuali - al fine di valutarne l'efficacia, l'efficienza e la coerenza con le esigenze di sicurezza dell'Ente.

L'aggiornamento del contenuto del DPS – scaturente dal verificarsi di mutamenti interni (tecnologici e/o organizzativi), dall'evolversi dello stato dell'arte delle tecnologie informatiche, dalla individuazione di vulnerabilità e criticità nello svolgimento delle normali operazioni, nonché da mutamenti normativi, sarà effettuato nei termini di legge ovvero entro il 31 marzo di ogni anno, con le stesse modalità previste per l'adozione.

Nota

Il presente documento e gli allegati in esso richiamati sono conservati in originale - quale parte integrante e sostanziale della deliberazione di Giunta camerale n. 20 del 22.03.2010 - presso l'Ufficio Segreteria e Protocollo.