Camera di Commercio di LUCCA

"Continuità operativa" - C.A.D. Art. 50 bis

Piano di Continuità Operativa ICT

Versione Documento	V1.1
Data emissione	_____
Redatto da :	Claudio Mori
Verificato da :	Giunta Camerale
Approvato da :	Delibera di Giunta _____
Autorizzato da :	Dr. Roberto Camisi – Segretario Generale Camera di Commercio di Lucca2014 Dr. Giorgio Bartoli - Presidente Camera di Commercio di Lucca2014

Con la collaborazione di :

"InfoCamere"

Società Consortile di Informatica delle Camere di Commercio Italiane per azioni

1. Storia delle Modifiche apportate PCO....4

2. Generalità 5

2.1 Premessa....5

2.1.1 Introduzione....5

2.1.2 Obiettivo del Piano di Continuità Operativa ICT....5

2.2 Scopo....6

2.3 Validità....6

2.4 Strategie....6

2.4.1 Gestione delle reperibilità....7

2.4.2 Formazione....7

2.5 Testing.... 8

2.5.1 Gestione ed aggiornamento del Piano di Continuità Operativa....8

3. Posizionamento del presente documento....8

3.1 Il percorso dello Studio di fattibilità Tecnica ex comma 4, art. 50-bis del CAD....8

3.2 Il parere di AgID....8

3.3 Variazione eventuale nel numero dei servizi e relative criticità....10

3.4 Definizioni....10

4. Siti nel Piano 13

5. Elenco Servizi 14

6. Piano di Continuità Operativa....19

6.1 Fase di reazione all'emergenza....19

6.1.1 Analizzare le criticità e dichiarare lo stato di crisi....19

6.1.2 Attivare il Centro di Controllo....20

6.1.3 Convocare il Comitato di Crisi....20

6.1.4 Informare il Consiglio Camerale e la Giunta della crisi in atto....20

6.1.5 Mettere in atto le misure di sicurezza per garantire l'accesso ai siti primario e/o secondario....20

6.1.6 Ordinare l'evacuazione del sito primario e verificare l'accessibilità del sito secondario....20

6.1.7 Valutare l'accessibilità ai sistemi e alle apparecchiature necessarie a garantire i servizi IT....21

6.1.8 Raccogliere tutti gli elementi necessari ad individuare il piano di soluzione della crisi....21

6.1.9 Valutare gli impatti sulle risorse infrastrutturali, economiche, umane e legali....21

6.1.10 Definire la soluzione da adottare....21

6.1.11 Attivare le comunicazioni interne ed esterne relative....22

6.2 Gestione dell'emergenza....22

6.2.1 Convocazione delle persone tecniche necessarie, eventuale trasferimento nel sito secondario....22

6.2.2 Comunicare ai fornitori la situazione di crisi e la necessità di dare supporto alla attivazione del sito....23

6.2.3 Attivazione del piano di Disaster Recovery Tecnologico, solo in caso di attivazione sito secondario....23

6.2.4 Eseguire il piano di DR (solo in caso di attivazione sito secondario) ed informare il Comitato di Crisi....23

6.3 Chiusura dell'emergenza....23

6.3.1 Comunicazione interna di chiusura della crisi con indicazione dei limiti imposti dalla situazione di crisi....24

6.3.2 Predisporre eventuale piano per il ripristino completo delle funzionalità....25

6.3.3 Comunicazione esterna chiusura crisi....25

7. Teams, Positions e Risorse....26

7.1 Comitato di crisi....26

7.2 Retrosportello.....26

7.3 Sportello.....27

7.4 Team operativo di Disaster Recovery.....28

7.5 Ufficio Stampa.....28

8. Fornitori.....29

9. Riferimenti.....30

Piano di Disaster Recovery 39

1. Storia delle Modifiche apportate al PCO

Il servizio Certificati di origine per le merci esportate all'estero, erogato direttamente dalla Camera, o attraverso altri Fornitori

Classe di Servizi : CERTIFICATI DI ORIGINE		
Emissione dei certificati di origine per le merci esportate all'estero		
servizi componenti : – Certificati di Origine Merci	Fornitore :	**Camera di Commercio di Lucca**
	Tipologia utente :	Imprese
	Indice complessivo di criticità :	3
	Classe di criticità :	media
	Soluzione tecnologica :	TIER 2
	RPO :	24 ore
	RTO :	72 ore

è stato affidato, a partire dal 1 gennaio 2017, a InfoCamere

Classe di Servizi : VIGILANZA E CONTROLLO PRODOTTI, METROLOGIA LEGALE, CERTIFICATI DI ORIGINE MERCI		
Vigilanza e controllo sui prodotti e per la metrologia legale e rilascio dei certificati di origine delle merci		
servizi componenti : – Gestione Servizio Metrico [Eureka] – Gestione e rilevazione prezzi – Sistema di Vigilanza del Mercato [Vimer] – Certificati di origine merci [Cert'O]	Fornitore :	Infocamere SCpA
	Tipologia utente :	Eterogenea (Cittadini,Imprese,P.A.)
	Indice complessivo di criticità :	4
	Classe di criticità :	media
	Soluzione tecnologica :	TIER 4
	RPO :	24 ore
	RTO :	72 ore

Versione:	na	Data Versione:	gg / mm / aaaa
Descr. modifiche:	Il punto 2.5 del precedente PCO prevedeva la *verifica della presenza corretta cassetta di backup presso la **sede alternativa di Viareggio - Via Leònida Rèpaci, 16*** in relazione al recupero dei dati sul Server di rete che gestisce le cartelle condivise e il programma di Rilevazione delle Presenze. A partire dal 01/01/2017 la Camera di Commercio di Lucca affiderà ad Infocamere un servizio in Hosting di replica/ridondanza del Server di dominio che svolge anche attività di File Server sopra indicato. Pertanto l'attività di verifica sarà indirizzata sulla effettiva ridondanza del server.		
Motivazioni :	Infocamere SCPA è la società in house delle Camere di Commercio svolge per conto del sistema camerale attività di gestione della rete geografica (icrete) garantendone l'integrità e l'efficienza. Pertanto attività di recupero dati e disaster recovery si inseriscono all'interno della rete camerale e pertanto se gestite da Infocamere sono maggiormente **funzionali all'architettura informatica -informativa .**		

2. Generalità

2.1 Premessa

2.1.1 Introduzione

La continuità dei sistemi informativi rappresenta per le pubbliche amministrazioni, nell'ambito delle politiche generali per la continuità operativa dell'ente, un aspetto necessario all'erogazione dei servizi a cittadini e imprese e diviene uno strumento utile per assicurare la continuità dei servizi e garantire il corretto svolgimento della vita nel Paese.

Al riguardo e più in particolare l'articolo 50-bis del CAD aggiornato (che attiene alla "Continuità operativa") delinea gli obblighi, gli adempimenti e i compiti che spettano alle Pubbliche Amministrazioni, a Agenzia per l'Italia e al Ministro per la pubblica amministrazione e l'innovazione, ai fini dell'attuazione della continuità operativa:

1) In relazione ai nuovi scenari di rischio, alla crescente complessità dell'attività istituzionale caratterizzata da un intenso utilizzo della tecnologia dell'informazione, le PP.AA.. predispongono i piani di emergenza in grado di assicurare la continuità delle operazioni per il servizio e il ritorno alla normale operatività.

2) Il Ministro per la pubblica amministrazione e l'innovazione assicura l'omogeneità delle soluzioni di continuità operativa definite dalle diverse Amministrazioni e ne informa con cadenza almeno annuale il Parlamento.

3) A tali fini, le pubbliche amministrazioni definiscono:

   a) il Piano di Continuità Operativa, che fissa gli obiettivi e i principi da perseguire, descrive le procedure per la gestione della continuità operativa, anche affidate a soggetti esterni. Il piano tiene conto delle potenziali criticità relative a risorse umane, strutturali, tecnologiche e contiene idonee misure preventive. Le amministrazioni pubbliche verificano la funzionalità del piano di continuità operativa con cadenza biennale;

   b) il Piano di Disaster Recovery, che costituisce parte integrante di quello di continuità operativa di cui alla lettera a) e stabilisce le misure tecniche e organizzative per garantire il funzionamento dei centri di elaborazione dati e delle procedure informatiche rilevanti in siti alternativi a quelli di produzione.

   Agenzia per l'Italia, sentito il Garante per la protezione dei dati personali, definisce le linee guida per le soluzioni tecniche idonee a garantire la salvaguardia dei dati e delle applicazioni informatiche, verifica annualmente il costante aggiornamento dei piani di Disaster Recovery delle amministrazioni interessate e ne informa annualmente il Ministro per la Pubblica Amministrazione e l'innovazione.

4) I piani di cui al comma 3 sono adottati da ciascuna amministrazione sulla base di appositi e dettagliati studi di fattibilità tecnica; su tali studi è obbligatoriamente acquisito il parere di Agenzia per l'Italia.

2.1.2 Obiettivo del Piano di Continuità Operativa ICT

Il presente Piano di Continuità Operativa (in seguito PCO) adottato con Delibera di Giunta n. 80 del 04/12/2015 e inviato all'Agid in data 24/12/2015 – Prot. GDOC5_D_1294603 – con le modifiche apportate ed approvate con Delibera di Giunta n. __ del _____ descrive le modalità di intervento a fronte di emergenze ed eventi critici, intendendosi come tali eventi anomali eccezionali di cui più sotto si riporta la descrizione. Gli eventi anomali che coinvolgono i servizi forniti dalla Camera possono avere cause interne o esterne, possono inoltre esser correlati a servizi gestiti in totale autonomia dalla Camera di Commercio o a servizi di fornitori esterni alla Camera di Commercio.

Il PCO provvede ad elencare:

- le modalità operative previste dai contratti con i fornitori esterni per la soluzione di eventi anomali di loro competenza
- l'organizzazione e modalità di intervento della Camera di Commercio per la gestione di eventi anomali di specifica competenza della Camera di Commercio stessa.

2.2 Scopo

Scopo del presente documento è descrivere le modalità di attivazione, le responsabilità ed i contatti relativi al Processo di Gestione delle Emergenze e dello Stato di Crisi della Camera Commercio di LUCCA.

La prima versione del documento è stata approvata nel Comitato di Crisi del 30-11-2015, e sarà rivista più volte per far fronte alle variazioni organizzative che occorreranno nel corso del tempo.

A partire da questa versione, il documento viene prodotto con uno specifico strumento di Business Continuity Management (Sungard), fornito da InfoCamere; lo strumento consente la registrazione di tutte le componenti necessarie alla realizzazione dei piani di continuità ed alla produzione di piani di lavoro specifici per i ruoli previsti.

2.3 Validità

Destinatari del Piano di Continuità Operativa della Camera Commercio di LUCCA, ciascuno per la parte di competenza, sono:

- i vertici dell'Amministrazione;
- il responsabile della CO, figura prevista nelle "Linee guida per il DR delle PA" emesso dall'Agenzia per l'Italia Digitale il 26 novembre 2011; per la Camera Commercio di LUCCA il ruolo è svolto dal **Sig. Claudio MORI**, nominato con determinazione dirigenziale n° 295/03-10-2014.
- il personale dell'Amministrazione di qualunque tipologia (fruitore o gestore) direttamente coinvolto nell'IT dell'Amministrazione;
- la comunità di riferimento territoriale e sociale (cittadini, imprese e associazioni di categoria) dell'Amministrazione;

- le organizzazioni e/o istituzioni che interagiscono con l'Amministrazione in modalità informatiche;
- se presenti, tutti i fornitori, a qualunque titolo, di attività di supporto informatico.

2.4 Strategie

I principi che stabiliscono le priorità nella gestione dell'emergenza, e che orientano le decisioni, sono:

- proteggere la vita e l'incolumità delle persone;
- prevenire ulteriori conseguenze derivanti dall'incidente di origine;
- garantire la continuità del servizio e tutelare il patrimonio di immagine della P.A.;
- salvaguardare i beni di cui la P.A. ha la disponibilità o la responsabilità;
- salvaguardare l'ambiente.

Tali principi sono coerenti con le normative vigenti (vedi cap. 9 Riferimenti).

Benché il presente Piano rappresenti una specifica realizzazione nel contesto di quanto previsto dall'art. 50-bis del CAD e non sia, quindi, direttamente riconducibile ad un preciso standard, sono norme internazionali di riferimento le norme ISO indicate nei riferimenti Relativamente al coinvolgimento di fornitori esterni per la realizzazione di soluzioni tecniche previste si ottempererà secondo normativa vigente (Dlgs. 12 aprile 2006 n. 163 e s.m.i. e DPR n. 207/2010).

2.4.1 Gestione delle reperibilità

Sono sempre reperibili i dirigenti, sia il **dott. Roberto CAMISI**, Segretario Generale dell'Ente, sia il **Sig. Claudio MORI**, Responsabile della Continuità Operativa.

Relativamente alle strutture tecniche indicate al cap. 7 "Teams, Positions e Risorse", la reperibilità è organizzata come segue:

- nel fine settimana (ven sab dom) è reperibile un addetto a rotazione all'interno del gruppo composto da "ufficio tecnico e patrimonio" e "ufficio servizi informatici" nel loro complesso.

2.4.2 Formazione

Le procedure previste per la Continuità Operativa saranno divulgate nelle seguenti modalità:

- nella versione originale presso i componenti del Comitato di Crisi, con incontro annuale per descrivere le eventuali implementazioni intervenute e verificare la congruenza del piano con le persone coinvolte
- formazione specifica sarà seguita dal personale tecnico che deve gestire il ripristino dei sistemi e la gestione della sede alternativa

- nota informativa, che sarà diffusa presso tutto il personale per renderlo edotto dell'esistenza di un PCO e delle modalità di coinvolgimento dei singoli uffici in detto piano

2.5 Testing

Il test periodico prevede:

- riunione annuale del comitato di crisi per aggiornare il comitato sulle modifiche eventualmente apportate al piano (su proposta del Responsabile del Comitato di Crisi)
- verifica effettiva ridondanza del server - domain controller e file server – con indirizzo IP 10.60.5.1 con il server in hosting presso InfoCamere SCPA.

2.5.1 Gestione ed aggiornamento del Piano di Continuità Operativa

➢ **Modalità di esecuzione dei test periodici**

Le stazioni della sede alternativa di Viareggio sono normalmente utilizzate per attività di sportello e retrosportello, non necessitano quindi di test specifici.

➢ **Modalità di revisione e adeguamento del piano**

Il documento viene rivisto dal RCO:

- a fronte di modifiche su sistemi/procedure di ripristino
- a fronte di sostituzione dell'elenco persone citate nel piano

Eventuali migliorie o modifiche significative del piano di continuità operativa vengono proposte dal RCO al Comitato di Crisi nella prevista riunione annuale o in apposita riunione convocata qualora se ne presenti la necessità

3. Posizionamento del presente documento

3.1 Il percorso dello Studio di fattibilità Tecnica ex comma 4, art. 50-bis del CAD

Lo Studio di Fattibilità Tecnica è stato inviato dalla Camera Commercio di LUCCA ad AgID in data 04/11/2014, Prot. n. 15045.

3.2 Il parere di AgID

Nel parere n. **1003/2015** emesso da parte di AgID il **23-01-2015**, ed inviato alla Camera Commercio di LUCCA il 26-01-2015 con Prot n. **0001007** , si esprime quanto segue:

CONSIDERATO

1. Considerazioni generali di natura strategica

1.1 Coerenza dell'iniziativa di DR con gli obiettivi complessivi che l'Amministrazione si propone di raggiungere ai fini della digitalizzazione e dell'attuazione degli adempimenti del CAD.

Relativamente alle attività rappresentate nella relazione dell'Amministrazione, si rileva che le soluzioni di DR delineate appaiono compatibili e congruenti con le iniziative e gli obiettivi dichiarati dalla Camera di Commercio di Lucca per l'attuazione del CAD e la digitalizzazione dei procedimenti amministrativi.

2. Analisi tecnica SFT e soluzione di DR proposta/adottata

2.1 Osservazioni sull'autovalutazione delle esigenze di salvaguardia dei dati e delle applicazioni delle Amministrazioni.

Si rileva che l'Amministrazione ha effettuato l'autovalutazione con il tool fornito dalla Agenzia per l'Italia Digitale esaminando i servizi in coerenza con il percorso indicato per la predisposizione dello SFT. Il numero di servizi sottoposto alla autovalutazione è pari a 18.

L'Amministrazione ha posto n. 3 servizi fuori ambito.

Al riguardo, si richiede che l'Amministrazione adotti almeno qualche modalità di protezione dei dati dei servizi posti fuori ambito conservando, per esempio, copie multiple dei dati degli stessi presso il sito primario con opportuni requisiti di sicurezza e conservazione.

2.2 Osservazioni sulle soluzioni tecniche proposte

2.2.1 Adeguatezza tecnica delle soluzioni prescelte rispetto alle esigenze descritte dall'Amministrazione

L'Amministrazione dà indicazioni in merito al sito secondario, indicando la distanza di quest'ultimo dal sito primario; a tal proposito, si ricorda comunque all'Amministrazione, che la localizzazione del sito secondario deve essere determinata in modo da garantire la continuità operativa anche nel caso di disastri estesi, i quali potrebbero rendere contemporaneamente indisponibili i due siti.

Con riferimento alla scelta delle soluzioni di continuità operativa, si richiama l'attenzione dell'Amministrazione ai seguenti requisiti minimi da verificare:

- verifica delle caratteristiche minime del sito secondario. Al proposito, si rimanda a quanto descritto nel documento dell'Agenzia "I SERVIZI MINIMI ESSENZIALI PER L'ADOZIONE DELLE SOLUZIONI DI DISASTER RECOVERY", reperibile al link http://www.digitpa.gov.it/sites/default/files/Raccomandazioni_PROFILI%20MINIMI%20SERVIZI

%20DI%20DR_v_2_4_0.pdf “, relativamente al servizio “D3 - Sito di Disaster Recovery: aree CED

e aree attrezzate per i posti di lavoro”, con particolare riferimento all’allegato di questo servizio; benché queste caratteristiche siano specificatamente relative a requisiti da richiedere a fornitori esterni, si ritiene che gli stessi requisiti debbano essere adottati anche nella scelta di un sito secondario quale soluzione interna;

- l’evidenza della presenza nel Piano di CO del fornitore delle procedure di continuità relative ai servizi IT forniti dall’Amministrazione;
- l’evidenza dell’effettivo svolgimento da parte dell’Amministrazione e del fornitore di un test almeno annuale con la presenza di personale dell’Amministrazione;
- la coerenza dei livelli di servizio relativi a RPO e RTO delle soluzioni tecniche con quanto indicato nella valutazione della criticità.

Si ricorda che il tool di autovalutazione fornisce delle indicazioni di massima e orientative sui Tier delle soluzioni tecniche da adottare. Si invita l’Amministrazione a richiedere contrattualmente, al fornitore della soluzione di DR, di rispondere alle esigenze di continuità operativa dell’Amministrazione, con particolare riferimento ai tempi massimi di ripristino (RTO) e di perdita massima di dati accettata (RPO).

Con riferimento alle soluzioni tecniche per i servizi forniti esternamente, proprio per il coinvolgimento di questi ultimi, si richiama l’Amministrazione alla verifica di questa scelta sotto il profilo della normativa vigente (Dlgs 12 aprile 2006 n. 163 e s.m.i e DPR n. 207/2010).

Si richiede all’Amministrazione, prima di dare seguito all’avviamento delle attività per la realizzazione delle soluzioni, di verificare che le soluzioni identificate siano coerenti con gli indirizzi prospettati dalle Linee Guida per la razionalizzazione della infrastruttura digitale della PA (http://www.agid.gov.it/sites/default/files/linee_guida/linee-guida- razionalizzazione-ced.pdf). Nel caso fossero necessarie informazioni per quanto sopra, è possibile inviare la richiesta per le stesse all’indirizzo: continuità_operativa@agid.gov.it.

Si ricorda, comunque, il ruolo che le Regioni rivestono ai fini delle richiamate Linee Guida.

2.2.2 Conformità della soluzione rispetto al percorso descritto nelle Linee Guida per il Disaster Recovery delle Pubbliche Amministrazioni”, emanate da DigitPA

L’Amministrazione ha seguito il percorso indicato nelle Linee Guida per il Disaster Recovery delle Pubbliche Amministrazioni e la circolare DigitPA n. 58/2011.

Si richiama l’attenzione dell’Amministrazione sull’avvenuta pubblicazione dell’aggiornamento 2013 delle Linee Guida, reperibili sul sito dell’Agenzia. In particolare, si sottolinea, in questo aggiornamento, la presenza di un modello di piano di continuità (http://www.agid.gov.it/sites/default/files/documenti_indirizzo/modello-pco-per- pa.pdf) specificatamente realizzato per il contesto delle Pubbliche Amministrazioni.

2.2.3 Valutazione delle eventuali differenze emerse fra la soluzione prescelta e quella che emerge dall’autovalutazione.

Tenuto conto dell’esito del percorso di autovalutazione, l’Amministrazione propone di realizzare 5 soluzioni: la soluzione tecnologica Tier 4/IC-A, la Tier 4/IC-B, la Tier 4/IC-C, la Tier 4/CCIAA-A e la Tier 3/CCIAA-B. Tali soluzioni sono coerenti e migliorative, rispetto ai Tier suggeriti dal tool di autovalutazione.

2.2.4 Valutazione dell'omogeneità delle soluzioni prescelte rispetto a quelle di altre Amministrazioni

La soluzione prevista dalla Camera di Commercio di Lucca è omogenea a quella di altre amministrazioni simili.

2.3. Osservazioni e eventuali suggerimenti di natura giuridico-amministrativa in merito ai tempi e modalità di realizzazione delle soluzioni, indicate dall'Amministrazione

Si prende atto dei tempi stimati da e si ricorda, comunque, quanto disposto rispetto ai tempi entro i quali è necessaria la disponibilità del piano di CO ai sensi del comma 10 dell'art.57 del D.lgs. 235/2010.

PER QUESTI MOTIVI

ai sensi dell'art. 50 bis (Continuità Operativa) del "Codice dell'Amministrazione Digitale", D.lgs. n. 82/2005 così come modificato dal D.lgs. 235/2010

esprime

parere favorevole, a condizione che:

1) l'Amministrazione verifichi la piena coerenza fra le soluzioni identificate e gli indirizzi prospettati dalle Linee Guida dei CED;

2) l'Amministrazione, relativamente ai servizi posti fuori ambito, verifichi l'opportunità di adottare, anche minime, modalità di salvaguardia dei dati;

3) relativamente alle soluzioni tecniche, venga verificato che la scelta del sito secondario sia adeguata a garantire le esigenze di continuità operativa a fronte di eventi che possano compromettere l'operatività di entrambi i siti e se ne dia riscontro nel piano di Disaster Recovery;

4) relativamente alle soluzioni tecnologiche Tier 4 / CCIAA-A e Tier 3 / CCIAA-B, l'Amministrazione non riferisce alcune informazioni dichiarando che verranno definite a contratto; al riguardo, si richiede, pertanto, che venga dato riscontro all'Agenzia non appena definiti questi dati;

5) le soluzioni tecniche di continuità operativa siano coerenti con i requisiti definiti in fase di autovalutazione e vengano verificati i requisiti sopraindicati per le soluzioni indicate;

6) venga verificato, nell'implementazione delle soluzioni tecniche di DR descritte, che le stesse siano effettivamente in grado di rispondere alle esigenza di CO con particolare riferimento ai tempi massimi di ripristino (RTO) e di perdita massima di dati accettata (RPO);

7) relativamente al coinvolgimento di fornitori esterni per l'implementazione delle soluzioni tecniche individuate dall'Amministrazione, si richiama quest'ultima alla verifica di questa scelta sotto il profilo della normativa vigente (Dlgs 12 aprile 2006 n. 163 e s.m.i. e DPR n. 207/2010).

3.3 Variazione eventuale nel numero dei servizi e relative criticità

Per i seguenti servizi, elencati come "in ambito" nello Studio di Fattibilità Tecnica, sono intervenute le seguenti variazioni rispetto a quanto indicato nello Studio stesso:

- **Sistema rilevazione presenze**: risiede sul server interno e pertanto i dati sono oggetto di backup giornaliero.
  Inoltre è stato attivato un servizio ridondante in hosting con Infocamere SCPA che replica in maniera totale il server interno.
  In caso di situazione di crisi basterà attivare il server presso Infocamere. La Camera di

Commercio ritiene di poter gestire una situazione di emergenza attraverso la registrazione manuale delle firme in entrata e in uscita dei dipendenti.

- **Sito Istituzionale, Gestione Delibere/Determine, Intranet interna**: lo SFT prevedeva una soluzione tecnologica Tier 4. Verificata la difficoltà del fornitore nel garantire una soluzione tecnologica Tier 4 e considerato che la soluzione minima richiesta (da autovalutazione) per il servizio in oggetto è Tier 2, la Camera di Commercio di Lucca ritiene di poterne gestire la C.O. con una soluzione Tier 2.

3.4 Definizioni

Termine / Acronimo	Definizione
Centro di Controllo	Luogo di riunione dei gruppi: – Comitato di Crisi / Emergenza – Team di Coordinamento di Crisi / Emergenza
Crisi	Si intende come crisi una situazione grave che impedisce la continuità del Business, per la cui gestione è richiesta l'attivazione del processo di Gestione della Crisi che prevede il coinvolgimento dei Vertici aziendali, l'utilizzo dei piani di Disaster Recovery o continuità operativa per il ripristino
Emergenza	Si intende come emergenza una situazione anomala per la risoluzione della quale è richiesto l'utilizzo di poteri, deleghe e procedure di ripristino non ordinarie, con gestione dell'incidente attraverso l'attivazione di figure / responsabilità specifiche e/o l'eventuale utilizzo di piani di continuità operativa per il ripristino
Incidente	Si intende come incidente una situazione anomala che ricade nell'esercizio a regime (probabilità alta / medio-alta di accadimento dell'evento), per la cui gestione è richiesto l'utilizzo delle policy vigenti, utilizzando nella maggior parte dei casi procedure consolidate, necessitando talvolta di analisi specifica e particolare attenzione.
Piano di Continuità Operativa ICT	Documento operativo che descrive tutte le attività e modalità finalizzate al ripristino, a seguito di un evento negativo di significativa rilevanza, che determini l'indisponibilità dei servizi classificati come "critici"
Piano di Disaster Recovery	Documento operativo che descrive tutte le attività necessarie a garantire, a fronte di un evento negativo di significativa rilevanza, che determini l'indisponibilità dei servizi definiti "critici", il ripristino degli stessi servizi, entro un arco temporale predefinito, tale da rendere, il più possibile, minime le interruzioni nell'erogazione dei servizi. Si evidenzia che il PDR è la sezione del PCO che descrive le attività di ripristino del sistema informativo.
RCO [Responsabile Continuità Operativa]	Il ruolo di RCO è quello di supportare l'Amministrazione per predisporre tutte le misure necessarie per ridurre l'impatto di un'emergenza ICT e reagire prontamente e in maniera efficace in caso di una interruzione delle funzioni ICT, a supporto dei servizi erogati, dovuta a un disastro. Inoltre ha la responsabilità' di sviluppare e mantenere aggiornato il PCO; il RCO e' membro del Comitato di crisi. Oltre ai compiti di cui si deve far carico durante la condizione di normalità operativa dell 'ICT, durante le situazioni che possono portare alla condizione di stato di emergenza ICT, il RCO svolge un ruolo fondamentale nella gestione dell'emergenza ICT, ed è impegnato in tutte le seguenti attività: – costituire il punto di riferimento/contatto per la segnalazione dello stato di emergenza ICT (reale o potenziale); – effettuare valutazioni qualitative e quantitative dell'impatto reale o potenziale che lo stato di emergenza ICT segnalato provoca/può provocare, individuando il personale, i servizi e gli utenti coinvolti per proporre al Comitato di Crisi la dichiarazione dello stato di emergenza; – richiedere la convocazione del Comitato di Crisi per la valutazione della dichiarazione dello stato di emergenza ICT, fornendo tutte le informazioni necessarie alle decisioni; – in caso di dichiarazione di emergenza ICT da parte del Comitato di Crisi coordinare i team operativi per la gestione dell'emergenza e per il processo di ritorno alla normalità; – aggiornare costantemente il Comitato di Crisi ICT durante le varie fasi di gestione dell'emergenza ICT; – informare il Comitato di Crisi della conclusione delle condizioni dell'emergenza ICT; – in caso di dichiarazione di conclusione dell'emergenza ICT da parte del Comitato di Crisi curare tutte le operazioni di ritorno alla normalità. Qualora la situazione di emergenza ICT si prolunghi oltre quanto previsto, il RCO deve valutare le azioni gestionali/comunicative, amministrative più opportune.
RPO [Recovery Point Object]	Rappresenta il massimo tempo che intercorre tra la produzione di un dato e la sua messa in sicurezza .

Termine / Acronimo	Definizione
RTO [Recovery Time Object]	Tempo atteso per il ripristino dei servizi critici sul sito di DR.
SCENARIO D1	Le condizioni cui far fronte sono: – Strumentazione tecnologica completamente inutilizzabile e/o isolata dal punto di vista della connettività di rete – Sede della Camera di Commercio di LUCCA inagibile (disastro strutturale / ambientale) A titolo di esempio si riporta una serie di eventi associati allo tipologia di scenario D1: – Alluvione estesa – Incendio esteso – Terremoto distruttivo
SCENARIO D2	Le condizioni cui far fronte sono: – Strumentazione tecnologica completamente inutilizzabile e/o isolata dal punto di vista della connettività di rete – Sede della Camera di Commercio di LUCCA agibile A titolo di esempio si riporta una serie di eventi associati allo tipologia di scenario D2: – Alluvione parziale – Crollo parziale della struttura – Mancanza di elettricità – Incendio – Perdita di connettività di rete
SCENARIO D3	Le condizioni cui far fronte sono: – Infrastruttura tecnologica parzialmente inutilizzabile – Sede della Camera di Commercio di LUCCA agibile A titolo di esempio si riporta una serie di eventi associati allo tipologia di scenario D3: – Allagamento parziale – Attacco informatico (malware) – Atti vandalici – Azioni di hacking – Caduta di un rack o computer – Errori umani – Furto – Guasti SW e/o HW – Guasto all'impianto di condizionamento – Incendio localizzato – Raptus di follia di personale interno – Eventi atmosferici
Sito Primario o Principale	Sito presso il quale sono collocate le infrastrutture tecnologiche di riferimento nelle normali condizioni operative
Sito Secondario o Alternativo	Sito presso il quale sono collocate le infrastrutture tecnologiche di riserva; può avere anche un ruolo secondario in situazione di normale operatività.
Ufficio servizi informatici	Personale coinvolto per interventi sulla rete, sui server e sugli apparati informatici
Ufficio tecnico e patrimonio	Personale coinvolto per interventi sugli impianti e sul patrimonio mobiliare e immobiliare, nonché per la logistica (facchinaggio, sgombro locali, movimentazione arredi ecc.)

Per ulteriori definizioni di termini ed espressioni che verranno utilizzati, ove non altrimenti specificato, si rimanda al "Glossario" contenuto nelle "Linee guida per il Disaster Recovery delle Pubbliche Amministrazioni".

4. Siti nel Piano

Denominazione Sito : CdC LUCCA – Sede centrale	
Location ID	001
Location type	Sede Primaria
Indirizzo	Corte Campana, 10 – 55100 Lucca
Telefono	
In caso di chiusura di questa sede tutti i servizi a cittadini, imprese e PP .AA. restano comunque disponibili con il canale internet, poiché servizi informatici resi da fornitori esterni, nei tempi e modi indicati nell'Elenco Servizi_generalità e Elenco Servizi_dettagli.	

Denominazione Sito : CdC LUCCA – Sede secondaria di Viareggio	
Location ID	002
Location type	Sede Secondaria
Indirizzo	Via Leònida Rèpaci, 16 – 55049 Viareggio
Telefono	

Si riportano le caratteristiche dettagliate di questa sede secondaria :

Infrastrutture di continuità e protezione fisica

L'armadio tecnologico è dotato di gruppo di continuità da 1000W, il raffreddamento avviene attraverso l'impianto termico condominiale, la sede è dotata di estintori per le procedure antincendio.

Controllo fisico degli accessi (impianti e procedure)

Nel caso di DR, le chiavi per l'accesso all'edificio ed ai locali utilizzati dalla Camera Commercio di LUCCA, sono a disposizione del Responsabile del DR e del Responsabile della sede di Viareggio.

Ambiente logistico (interno) per la continuità

Presso la sede di Viareggio è disponibile una stanza con 4 scrivanie e 4 postazioni di lavoro. Lo switch in dotazione presso questa sede ha 8 ingressi, è quindi possibile espandere il numero di postazioni

5. Elenco Servizi

➢ Servizi forniti da InfoCamere

Classe di Servizi : ALTRI REGISTRI, ALBI E RUOLI

Gestione delle iscrizioni e consultazione dei registri, albi, ruoli e repertori, non indicati nella classe 'Albi Camerali' tenuti o gestiti dalle Camere di Commercio con contributo obbligatorio

servizi componenti :
- Imprese operanti con l'estero - [ItalianCom]

Fornitore :	Infocamere SCpA
Tipologia utente :	Eterogenea (Cittadini,Imprese,P.A.)
Indice complessivo di criticità :	4
Classe di criticità :	media
Soluzione tecnologica :	TIER 4
RPO :	24 ore
RTO :	72 ore

Classe di Servizi : ARCHIVIO PARD E ALBI CAMERALI

Gestione dei documenti obbligatori per gli Albi la cui gestione informatica è affidata dai Consorziati alla Società Consortile InfoCamere Scpa

servizi componenti :
- Albi Camerali – [ALCA] - Albi e Ruoli Camerali
- Albi Camerali – [ALCA] - Gestione esami
- Artigiani - Albo Artigiani e Previdenza Artigiana

Fornitore :	Infocamere SCpA
Tipologia utente :	Eterogenea (Cittadini,Imprese,P.A.)
Indice complessivo di criticità :	4
Classe di criticità :	media
Soluzione tecnologica :	TIER 4
RPO :	4 ore
RTO :	72 ore

Classe di Servizi : CARTE TACHIGRAFICHE

Gestione del sistema informativo delle Camere di Commercio di cui al decreto del ministero delle attività produttive del 23 giugno 2005, degli strumenti elettronici e telematici necessari alla emissione, rilascio e gestione delle carte tachigrafiche in conformità con la normativa vigente

servizi componenti :
- Carte Tachigrafiche

Fornitore :	Infocamere SCpA
Tipologia utente :	Eterogenea (Cittadini,Imprese,P.A.)
Indice complessivo di criticità :	4
Classe di criticità :	media
Soluzione tecnologica :	TIER 4
RPO :	24 ore
RTO :	72 ore

Classe di Servizi : CONTABILITA', PIANIFICAZIONE, CONTROLLO DI GESTIONE E AMMINISTRAZIONE APERTA

Gestione dei documenti obbligatori per gli Albi la cui gestione informatica è affidata dai Consorziati alla Società Consortile InfoCamere Scpa

servizi componenti :
- Sistema Gestione Amministrazione del Personale [Sipert]
- Sistemi per la Gestione Amministrativo-Contabile
- Pubblicamera

Fornitore :	Infocamere SCpA
Tipologia utente :	Eterogenea (Cittadini,Imprese,P.A.)
Indice complessivo di criticità :	4
Classe di criticità :	media
Soluzione tecnologica :	TIER 4
RPO :	24 ore
RTO :	72 ore

Classe di Servizi : DIRITTO ANNUALE

Gestione riscossione del diritto annuale, dei diritti di segreteria e dell'imposta di bollo dovute ai Soci consorziati

servizi componenti :
- Diritto Annuale e sanzioni

Fornitore :	Infocamere SCpA
Tipologia utente :	Eterogenea (Cittadini,Imprese,P.A.)
Indice complessivo di criticità :	4
Classe di criticità :	media
Soluzione tecnologica :	TIER 4
RPO :	24 ore
RTO :	72 ore

Classe di Servizi : FACILITAZIONE GESTIONE ATTIVITA' CAMERALI

Procedure informatiche per lo svolgimento da parte delle Camere di Commercio dei propri compiti istituzionali in conformità alle normative vigenti ed alle disposizioni impartite dal Ministero dello Sviluppo Economico non considerati in classi specifiche

servizi componenti :
- Gestione Contributi Erogati dalle Camere [CERC]

Fornitore :	Infocamere SCpA
Tipologia utente :	Eterogenea (Cittadini,Imprese,P.A.)
Indice complessivo di criticità :	4
Classe di criticità :	media
Soluzione tecnologica :	TIER 4
RPO :	24 ore
RTO :	72 ore

Classe di Servizi : REGISTRO IMPRESE

Predisposizione, tenuta, conservazione e gestione del Registro delle Imprese e del Repertorio Economico Amministrativo (R.E.A.), ai sensi degli artt.1 e 8 della legge 29 dicembre 1993, n. 580

servizi componenti :
- Registro Imprese - Interrogazioni
- Registro Imprese - Pratiche
- Registro Imprese - Servizi per l'efficienza
- Registro Imprese - Istruttoria
- Registro Imprese - Servizi Statistici
- Registro Imprese - Elaborazioni batch
- registroimprese.it - Telemaco

Fornitore :	Infocamere SCpA
Tipologia utente :	Eterogenea (Cittadini,Imprese,P.A.)
Indice complessivo di criticità :	4
Classe di criticità :	media
Soluzione tecnologica :	TIER 4
RPO :	4 ore
RTO :	72 ore

Classe di Servizi : REGISTRO INFORMATICO DEI PROTESTI

La predisposizione, la tenuta, la conservazione e la gestione del Registro informatico dei Protesti, ai sensi dell'art.3bis della legge 15 novembre 1995, n.480

servizi componenti :
- Registro Informatico dei Protesti

Fornitore :	Infocamere SCpA
Tipologia utente :	Eterogenea (Cittadini,Imprese,P.A.)
Indice complessivo di criticità :	4
Classe di criticità :	media
Soluzione tecnologica :	TIER 4
RPO :	24 ore
RTO :	72 ore

Classe di Servizi : RETE TELEMATICA E SERVIZI DI CONNETTIVITA' (Internet e Posta Elettronica)

Gestione di un'unica rete telematica nazionale atta a collegare il centro elaborazione dati della Società Consortile con tutte le sedi principali dei Soci Consorziati, al fine di consentire la fruizione e l'erogazione di servizi informatici e l'accesso al servizio di connettività e di posta elettronica

servizi componenti :
- Servizi Internet – Intranet
- Posta Elettronica

Fornitore :	Infocamere SCpA
Tipologia utente :	Eterogenea (Cittadini,Imprese,P.A.)
Indice complessivo di criticità :	4
Classe di criticità :	media
Soluzione tecnologica :	TIER 4
RPO :	1 ora
RTO :	72 ore

Classe di Servizi : SANZIONI AMMINISTRATIVE

Sanzioni Amministrative erogate dalle CCIAA

servizi componenti :
- Sanzioni Amministrative [Accesa]

Fornitore :	Infocamere SCpA
Tipologia utente :	Eterogenea (Cittadini,Imprese,P.A.)
Indice complessivo di criticità :	4
Classe di criticità :	media
Soluzione tecnologica :	TIER 4
RPO :	24 ore
RTO :	72 ore

Classe di Servizi : SERVIZI DI CONCILIAZIONE E ARBITRATO

Gestione delle Conciliazioni e Arbitrato

servizi componenti :
- Mediazione Camerale [CONCILIA]

Fornitore :	Infocamere SCpA
Tipologia utente :	Eterogenea (Cittadini,Imprese,P.A.)
Indice complessivo di criticità :	4
Classe di criticità :	media
Soluzione tecnologica :	TIER 4
RPO :	24 ore
RTO :	72 ore

Classe di Servizi : SERVIZI DI GESTIONE DOCUMENTALE

Procedure informatiche per lo svolgimento da parte delle Camere di Commercio dei propri compiti istituzionali in tema di Gestione Documentale, Protocollazione e Conservazione Documentale

servizi componenti :
- Sistema di WorkFlow
- Sistema di Gestione Documentale [LegalCycle]

Fornitore :	Infocamere SCpA
Tipologia utente :	Eterogenea (Cittadini,Imprese,P.A.)
Indice complessivo di criticità :	4
Classe di criticità :	media
Soluzione tecnologica :	TIER 4
RPO :	4 ore
RTO :	72 ore

Classe di Servizi : SERVIZI PER L'AMBIENTE		
Servizi legati alla salvaguardia ambientale		
servizi componenti : – MUD - Modello Unico di dichiarazione Ambientale – RAEE - Registro Nazionale Trattamento Rifiuti di apparecchiature elettriche ed elettroniche – SISTRI - Sistema Tracciabilità Rifiuti – Albo Gestori Ambientali – Registro FGas – Pile	Fornitore :	Infocamere SCpA
	Tipologia utente :	Eterogenea (Cittadini,Imprese,P.A.)
	Indice complessivo di criticità :	4
	Classe di criticità :	media
	Soluzione tecnologica :	TIER 4
	RPO :	24 ore
	RTO :	72 ore

Classe di Servizi : VIGILANZA E CONTROLLO PRODOTTI, METROLOGIA LEGALE, CERTIFICATI DI ORIGINE MERCI		
Vigilanza e controllo sui prodotti e per la metrologia legale e rilascio dei certificati di origine delle merci		
servizi componenti : – Gestione Servizio Metrico [Eureka] – Gestione e rilevazione prezzi – Sistema di Vigilanza del Mercato [Vimer] – Certificati di origine merci [Cert'O]	Fornitore :	Infocamere SCpA
	Tipologia utente :	Eterogenea (Cittadini,Imprese,P.A.)
	Indice complessivo di criticità :	4
	Classe di criticità :	media
	Soluzione tecnologica :	TIER 4
	RPO :	24 ore
	RTO :	72 ore

➢ Servizi Servizi erogati direttamente dalla Camera, o attraverso altri Fornitori

Classe di Servizi : PRESENZE DEL PERSONALE		
Rilevazione delle presenze del personale camerale		
servizi componenti : – Rilevazione presenze del personale camerale	Fornitore :	**Camera di Commercio di Lucca**
	Tipologia utente :	Interno
	Indice complessivo di criticità :	3
	Classe di criticità :	media
	Soluzione tecnologica :	TIER 2
	RPO :	24 ore
	RTO :	72 ore

Classe di Servizi : SITO ISTITUZIONALE		
Pubblicità legale da esporre sul Sito Istituzionale Gestione della predisposizione degli Atti ufficiali della camera Intranet interna all'Ente		
servizi componenti : – Sito web istituzionale – Gestione Delibere/Determine – Gestione intranet	Fornitore :	**Lucense S.c.p.A.**
	Tipologia utente :	Eterogenea (Cittadini,Imprese,P.A.)
	Indice complessivo di criticità :	3
	Classe di criticità :	media
	Soluzione tecnologica :	TIER 2
	RPO :	24 ore
	RTO :	72 ore

6. Piano di Continuità Operativa

6.1 Fase di reazione all'emergenza

➢ **La struttura organizzativa**

La rilevazione di un evento con impatti ICT segue un iter di escalation così definito:

- Rilevazione incidente: l'ufficio informatico, se l'incidente blocca le attività per più di 3 ore avvisa il RCO. che decide se fare escalation e attivare il comitato di crisi
- Valutazione: il RCO valuta se procedere ad escalation comunicando il problema al management
- Attivazione del Comitato di Crisi: se il responsabile del Comitato della Continuità Operativa ritiene significativa la gravità dell'incidente, dà inizio all'attivazione del Comitato di Crisi

6.1.1 Analizzare le criticità e dichiarare lo stato di crisi

Tabella Responsabilità / Competenza	
RESPONSABILITA'	• Responsabile Continuità Operativa
COMPETENZA	

Verificare la richiesta di apertura Crisi / riscontrare lo Stato di Crisi e dichiarare lo Stato di Crisi

L'attivazione del comitato di crisi risulta necessaria almeno per le seguenti casistiche:

- Significativi impatti sull'erogazione di uno o più servizi
- Difficoltà nel reperire le risorse (tecnologiche/umane) necessarie/preposte alla risoluzione dei problemi
- Incertezza sui tempi di risoluzione
- Criticità di ripartenza
- Attacchi informatici
- Impatto mediatico e/o economico

Gli scenari di eventi disastrosi cui la Continuità Operativa intende far fronte sono:

- D1 - Disastro Grave
- D2 - Disastro Tecnologico
- D3 - Gravi Danni Parziali

In caso di disservizio, al cap. 5 "Elenco Servizi" sono riportati i fornitori delle varie classi di servizio censite dalla Camera di Commercio, in particolare:

- per i servizi fornitori da Infocamere si richiede ad Infocamere di intervenire secondo gli accordi contrattuali in essere riportati al cap. 8 "Fornitori".

- in caso di disservizi relativi ai servizi interni (File server ed Active Directory), si interviene con procedure interne alla Camera di Commercio di LUCCA, descritte in questo documento e suoi allegati.
- per il servizio "SITO ISTITUZIONALE", fornito dalla Società Lucense S.c.p.A, si richiede al fornitore di intervenire secondo gli accordi contrattuali in essere, sintetizzati al cap. 8 "Fornitori"..

6.1.2 Attivare il Centro di Controllo

Tabella Responsabilità / Competenza	
RESPONSABILITA'	• Ufficio Tecnico
COMPETENZA	

Attivare il Centro di Controllo, scegliendo tra le sedi alternative previste, comunicare la scelta al Responsabile della Continuità Operativa ed alle funzioni aziendali, individuate come necessarie alla soluzione della crisi, da parte del Comitato di Crisi.

6.1.3 Convocare il Comitato di Crisi

Tabella Responsabilità / Competenza	
RESPONSABILITA'	• Responsabile Continuità Operativa
COMPETENZA	

Convocare il Comitato di Crisi presso il Centro di Controllo

6.1.4 Informare il Consiglio Camerale e la Giunta della crisi in atto

Tabella Responsabilità / Competenza	
RESPONSABILITA'	• Responsabile Comunicazione
COMPETENZA	

Inviare nota al Consiglio Camerale ed alla Giunta

6.1.5 Mettere in atto le misure di sicurezza per garantire l'accesso ai siti primario e/o secondario

Tabella Responsabilità / Competenza	
RESPONSABILITA'	• Ufficio Tecnico
COMPETENZA	

Mettere in atto le misure di sicurezza o di protezione necessarie per garantire l'incolumità delle persone e rilasciare l'autorizzazione al sopralluogo del sito.

Predisporre una documentazione, anche fotografica, dei danni subiti.

Definire le misure atte a garantire l'incolumità fisica delle persone che accedono al sito primario.

6.1.6 Ordinare l'evacuazione del sito primario e verificare l'accessibilità del sito secondario

Tabella Responsabilità / Competenza	
RESPONSABILITA'	• Ufficio Tecnico
COMPETENZA	

Definire le nuove misure straordinarie per l'accesso al sito primario o ordinare l'evacuazione del sito primario.

Effettuare una verifica preliminare dell'accessibilità del sito secondario.

6.1.7 Valutare l'accessibilità ai sistemi e alle apparecchiature necessarie a garantire i servizi IT

Tabella Responsabilità / Competenza	
RESPONSABILITA'	• Responsabile Continuità Operativa
COMPETENZA	

Eseguire una approfondita valutazione dei sistemi del sito primario e produrre un rapporto nel quale indicare:

- i principali rischi individuati ed eventuali politiche preliminari per la loro minimizzazione;
- le aree che dovranno essere monitorate per la sicurezza ed integrità dell'IT.

Richiedere eventuali valutazioni aggiuntive specifiche ad esperti esterni.

Attivare la Procedura di Comunicazione.

6.1.8 Raccogliere tutti gli elementi necessari ad individuare il piano di soluzione della crisi

Tabella Responsabilità / Competenza	
RESPONSABILITA'	• Ufficio Servizi Informatici
COMPETENZA	• Ufficio Tecnico

Sulla base dell'analisi dei danni subiti, identificare i principali rischi informatici ed infrastrutturali inerenti il ripristino della Continuità Operativa e valutare il costo delle contromisure e la riduzione attesa del livello di rischio.

Determinare il livello di rischio che l'organizzazione intende accettare confrontandolo con il costo associato. Sulla base di questa decisione il Comitato individua le possibili strategie per il ripristino.

Valutare gli impatti dei disservizi causati agli utenti.

6.1.9 Valutare gli impatti sulle risorse infrastrutturali, economiche, umane e legali

Tabella Responsabilità / Competenza	
RESPONSABILITA'	• Responsabile Continuità Operativa
COMPETENZA	

Verificare la effettiva disponibilità delle persone necessarie per la attivazione del Sito Secondario (vedi cap. 7 "Teams, Positions e Risorse").

Controllare eventuali implicazioni legali derivanti dai disservizi causati e definire la strategia e le azioni per minimizzare gli eventuali rischi legali.

Verificare le attività necessarie per l'attivazione della infrastruttura IT del Sito Secondario, considerando l'effettivo allineamento tecnologico e informativo.

Analizzare le informazioni prodotte nei passi precedenti, in particolare l'analisi dei Rischi, ed il grado di allineamento del Sito Secondario.

6.1.10 Definire la soluzione da adottare

Tabella Responsabilità / Competenza	
RESPONSABILITA'	• Responsabile Continuità Operativa
COMPETENZA	• Referente Ufficio Servizi Informatici • Referente Ufficio tecnico • Responsabile Coordinamento • Responsabile Servizio di Prevenzione e Protezione • Segretario Generale

Decidere se attivare il sito secondario (Contigency Plan) oppure riattivare il sito primario oppure intraprendere altre soluzioni.

Le azioni previste dovranno includere:

- Predisposizione di stazioni di lavoro (Ufficio Servizi Informatici - Referente Informatico Infocamere)
- Eventuali spese di funzionamento urgenti (RCO - Provveditore)
- Supporto logistico (Ufficio Tecnico)

6.1.11 Attivare le comunicazioni interne ed esterne relative

Tabella Responsabilità / Competenza	
RESPONSABILITA'	• Responsabile Comunicazione
COMPETENZA	

Attivare la Procedure di Comunicazione per diffondere la conoscenza di modifiche nei servizi forniti.

In caso di emergenza, presso la sede di Viareggio si offrono all'utenza, con orario ampliato e con personale aggiuntivo, i seguenti servizi:

- Sportello del Registro delle imprese
- Retrosportello del Registro delle Imprese (rispetto del termine dei 5 gg. per esame pratiche). Il servizio Retrosportello del Registro delle Imprese (rispetto del termine dei 5 gg. per esame pratiche) può essere erogato anche attraverso collegamenti in VPN – Telelavoro
- Certificati del commercio estero
- Carte tachigrafiche e CNS

Gli altri servizi saranno resi operativi in tempi successivi.

Dettaglio attività previste:

- Avvisare sede Viareggio (RCO - Responsabile sede Viareggio)
- Info su nuovo orario Viareggio e chiusura LUCCA (RCO)

6.2 Gestione dell'emergenza

Questa fase permette di attivare il sito alternativo.

6.2.1 Convocazione delle persone tecniche necessarie, eventuale trasferimento nel sito secondario

Tabella Responsabilità / Competenza	
RESPONSABILITA'	• Responsabile Continuità Operativa
COMPETENZA	

Convocazione del Team Operativo, verifica che tutti i ruoli necessari siano ricoperti con sostituzioni in caso di necessità. La convocazione termina con l'arrivo nel punto di raccolta concordato di tutto il personale necessario.

Si tiene l'incontro di kick-off nel corso del quale: si illustrano le principali attività da realizzare, si forniscono le politiche di sicurezza informatica, si segnalano eventuali rischi e problemi a cui occorre prestare particolare attenzione.

Viene validata la parte di propria competenza per l'attivazione del Contingency Plan, si approvano le azioni individuate da parte del Comitato di Crisi.

6.2.2 Comunicare ai fornitori la situazione di crisi e la necessità di dare supporto alla attivazione del sito

Tabella Responsabilità / Competenza		
RESPONSABILITA'	•	Responsabile Continuità Operativa
COMPETENZA	•	Referente Ufficio Servizi Informatici

Contattare i principali fornitori per avvertirli della crisi aziendale e richiedere loro la disponibilità a fornire una corsia preferenziale ad eventuali richieste dovessero rendersi necessarie.

Per l'elenco fornitori si rimanda al cap. 8 "Fornitori"

6.2.3 Attivazione del piano di Disaster Recovery Tecnologico, solo in caso di attivazione sito secondario

Tabella Responsabilità / Competenza		
RESPONSABILITA'	•	Responsabile Continuità Operativa
COMPETENZA		

Attivare il Contingency Plan (Piano DR) Da questo momento inizia il conteggio del RTO (tempo atteso per il ripristino dei servizi critici).

Eseguire le attività di ripristino in Piano.

Controllare lo stato avanzamento delle attività del Contingecy Plan.

Informare il Comitato di Crisi sull'avanzamento delle attività, sulle previsioni di riattivazione, sul rispetto del piano prestabilito.

Nel caso sia necessari attivare la sede alternativa di Viareggio dovranno esser coinvolte le persone che coprono i seguenti ruoli:

- Provveditore
- Ufficio Informatico
- Ufficio Tecnico
- Responsabile della sede di Viareggio

i relativi nominativi sono individuabili nel cap. 7 “Teams, Positions e Risorse”.

Il trasporto dei dipendenti verso la sede secondaria di Viareggio avviene con mezzi scelti dal dipendente (privati o pubblici) senza organizzazione da parte dell’Ente.

6.2.4 Eseguire il piano di DR (solo in caso di attivazione sito secondario) ed informare il Comitato di Crisi

Tabella Responsabilità / Competenza		
RESPONSABILITA'	•	Referente Ufficio Servizi Informatici
COMPETENZA		

Comunicare i tempi di completamento del piano di DR, il servizio potrà riprendere anche in mancanza del File Server / Active Directory ma è necessario provvedere alla sua predisposizione presso il sito secondario, dovrà esser comunicata la data entro cui si prevede il rilascio del server

presso la sede alternativa.

Verificare il rispetto del RTO.

6.3 Chiusura dell'emergenza

Con questa fase si completa l'attivazione del sito alternativo per riprendere il servizio in modo ridotto, la fase si conclude con indicazione dei limiti imposti dall'emergenza e una sommaria definizione dei successivi interventi necessari alla ripresa completa del servizio.

6.3.1 Comunicazione interna di chiusura della crisi con indicazione dei limiti imposti dalla situazione di crisi

Tabella Responsabilità / Competenza	
RESPONSABILITA'	• Responsabile Continuità Operativa
COMPETENZA	

Comunicare al Comitato di Crisi il completamento del Ripristino operativo e formalizzare, in un rapporto, i limiti che la situazione operativa comporta (servizi disponibili, disallineamenti, livelli di servizio, etc)

Comunicare al personale di Sportello e di Retrosportello la necessità di presentarsi alla sede di Viareggio

Comunicare al personale non coinvolto l'impossibilità di accedere allo stabile di LUCCA

Presso la sede di Viareggio, che verrà usata come sede alternativa in caso di indisponibilità della sede primaria dell'ente, sarà rispettato il seguente orario di apertura per il pubblico:

Sportello informazioni Registro imprese / Artigianato / Deposito Bilanci

- Lunedì, Mercoledì e Venerdi dalle ore 9,00 alle ore 13,00
- Lunedì e Mercoledì pomeriggio: dalle ore 15.00 alle ore 16.00

Deposito domande e Informazioni Marchi e Brevetti
Solo su appuntamento

- da Lunedì a Venerdì: dalle ore 9.00 alle ore 13.00
- Lunedì e Mercoledì: pomeriggio dalle ore 15.00 alle ore 16.00

Ufficio Ispettivo (metrico)

- Lunedì e Mercoledì: dalle ore 9,00 alle ore 13,00; dalle ore 15,00 alle ore 16,00
- Venerdì: dalle ore 9,00 alle ore 13,00

Sportello Nuova impresa e finanziamenti - Ufficio Sviluppo Imprenditoriale

- Lunedì, martedì, giovedì e venerdì: su appuntamento dalle 9.00 alle 13.00
- Mercoledì: chiuso
- Lunedì pomeriggio: su appuntamento dalle 15.00 alle 16.00

Tutti gli altri Sportelli

- da Lunedì a Venerdì: dalle ore 9.00 alle ore 13.00
- Lunedì e Mercoledì: pomeriggio dalle ore 15.00 alle ore 16.00

L'informazione agli utente per quanto sopra (la chiusura della sede primaria e il nuovo orario della sede di Viareggio) sarà comunicata dall'ufficio stampa.

6.3.2 Predisporre eventuale piano per il ripristino completo delle funzionalità

Tabella Responsabilità / Competenza	
RESPONSABILITA' COMPETENZA	• Responsabile Continuità Operativa

Per fronteggiare casi di prolungata indisponibilità (superiore a 3 settimane) della sede primaria, la Camera di Commercio di Lucca valuterà soluzioni alternative che comprendono possibili accordi di "mutuo soccorso" (come previsto nell'ultima versione delle Linee guida per la redazione del Piano Disaster Recovery, emanate dall'Agenzia Italia Digitale AGID) con altre Camere di Commercio che prevedono la messa a disposizione reciproca (qualora l'impossibilità ad utilizzare la propria sede principale persista per più di 3 settimane) almeno 5 stazioni di lavoro attrezzate per le procedure Infocamere (contabilità, atti).

6.3.3 Comunicazione esterna chiusura crisi

Tabella Responsabilità / Competenza	
RESPONSABILITA' COMPETENZA	• Responsabile Comunicazione

Comunicare al Consiglio Camerale e alla Giunta i limiti imposti dalla situazione di crisi ed il fatto che siano in corso azioni aggiuntive per individuare le azioni opportune.

Presso la sede di Viareggio, che verrà usata come sede alternativa in caso di indisponibilità della sede primaria dell'ente, sarà rispettato il seguente orario di apertura per il pubblico:

Sportello informazioni Registro imprese / Artigianato / Deposito Bilanci

- Lunedì, Mercoledì e Venerdi dalle ore 9,00 alle ore 13,00
- Lunedì e Mercoledì pomeriggio: dalle ore 15.00 alle ore 16.00

Deposito domande e Informazioni Marchi e Brevetti
Solo su appuntamento

- da Lunedì a Venerdì: dalle ore 9.00 alle ore 13.00
- Lunedì e Mercoledì: pomeriggio dalle ore 15.00 alle ore 16.00

Ufficio Ispettivo (metrico)

- Lunedì e Mercoledì: dalle ore 9,00 alle ore 13,00; dalle ore 15,00 alle ore 16,00
- Venerdì: dalle ore 9,00 alle ore 13,00

Sportello Nuova impresa e finanziamenti - Ufficio Sviluppo Imprenditoriale

- Lunedì, martedì, giovedì e venerdì: su appuntamento dalle 9.00 alle 13.00
- Mercoledì: chiuso
- Lunedì pomeriggio: su appuntamento dalle 15.00 alle 16.00

Tutti gli altri Sportelli

- da Lunedì a Venerdì: dalle ore 9.00 alle ore 13.00
- Lunedì e Mercoledì: pomeriggio dalle ore 15.00 alle ore 16.00

L'informazione agli utente per quanto sopra (la chiusura della sede primaria e il nuovo orario della sede di Viareggio) sarà inviata ai mass-media locali, nonché pubblicata sul sito

7. Teams, Positions e Risorse

7.1 Comitato di crisi

Il comitato di gestione della crisi si incarica di analizzare le situazioni anomale ed individuare le corrette reazioni sulla base di informazioni riportate dai suoi componenti e da loro eventuali riporti

Il comitato di gestione della crisi, definito nella Determina num. n. 295 del 03/10/2014, è così costituito:

COGNOME	NOME	UFFICIO COMPETENTE	WORK PHONE	MOBILE
Bruni	Alessandra	Dirigente Settore Anagrafico e Regolazione del Mercato	0583976648	3389462182
Camisi	Roberto	Segretario Generale	0583976647	3293606491
Granucci	Luca	Provveditore	0583976614	
Marsili	Massimo	Dirigente Area Amministrazione e Personale	0583976438	3389326971
Mori	Claudio	Responsabile Continuità Operativa	0583976612	3473663384

7.2 Retrosportello

Le persone che svolgono attività di Retrosportello necessarie a garantire le funzionalità minime della Camera di Commercio anche in situazioni di crisi.

COGNOME NOME	UFFICIO COMPETENTE	WORK PHONE	MOBILE
Salani Manuela	Registro delle Imprese	0583976424	
Bianchi Marinella	Registro delle Imprese	0583976603	
Giampaoli Monica	Registro delle Imprese	0583976412	
Giannini Laura	Registro delle Imprese	0583976611	
Giungato Isabella	Registro delle Imprese	0583976618	
Gregori Massimo	Registro delle Imprese	0583976654	

COGNOME NOME	UFFICIO COMPETENTE	WORK PHONE	MOBILE
Manca Nicoletta	Registro delle Imprese	0583976420	
Martinelli Stefano	Registro delle Imprese	0583976644	
Meccariello Claudio	Registro delle Imprese	0583976404	
Raffaelli Paola	Registro delle Imprese	0583976650	
Rizzuti Raffaella	Registro delle Imprese	0583976653	
Sciortino Mariarosa	Registro delle Imprese	0583976303	
Spinelli Maria Cristina	Registro delle Imprese	0583976302	
Stagi Luca	Registro delle Imprese	0583976608	
Pasquini Marco	Artigianato, Protesti, Documenti Export	0583976601	
Barbieri Nicola	Artigianato, Protesti, Documenti Export	0583976304	
Barsetti Monica	Artigianato, Protesti, Documenti Export	0583976662	
Bianchi Romina	Artigianato, Protesti, Documenti Export	0583976663	
Clemente Maurizio	Artigianato, Protesti, Documenti Export	0583976669	
Giannotti Romana	Artigianato, Protesti, Documenti Export	0583976620	
Golia Maria Luisa	Artigianato, Protesti, Documenti Export	0583976606	
Martini Enrica	Artigianato, Protesti, Documenti Export	0583976605	
Salvetti Olga	Artigianato, Protesti, Documenti Export	0583976672	
Giovannini Morena	Diritto Annuale	0583976685	
Dal Porto Carla	Diritto Annuale	0583976418	
Della Nina Paolo	Brevetti e Funzioni ispettive	0583976627	
Saraff Alessandro	Brevetti e Funzioni ispettive	0583976635	
Pedone Anna Maria	Arbitrato e Conciliazione	0583976692	
Lotti Enrica	Arbitrato e Conciliazione	0583976645	

COGNOME NOME	UFFICIO COMPETENTE	WORK PHONE	MOBILE
Palla Stefano	Arbitrato e Conciliazione	0583976641	
Pedreschi Milena	Arbitrato e Conciliazione	0583976434	
Galli Silvia	Segreteria e Protocollo	0583976655	
Ferti Francesca	Segreteria e Protocollo	0583976413	
Baldocchi Mauro	Segreteria e Protocollo	0583976668	
Francesca Sargenti	Relazione con l'Esterno	0583976686	
Vecchi Delia	Relazione con l'Esterno	0583976661	

7.3 Sportello

Le persone che svolgono attività di Sportello necessarie a garantire le funzionalità minime della Camera di Commercio anche in situazioni di crisi.

COGNOME NOME	UFFICIO COMPETENTE	WORK PHONE	MOBILE
Salani Manuela	Registro delle Imprese	0583976424	
Bianchi Marinella	Registro delle Imprese	0583976603	
Giampaoli Monica	Registro delle Imprese	0583976412	
Giannini Laura	Registro delle Imprese	0583976611	
Giungato Isabella	Registro delle Imprese	0583976618	
Gregori Massimo	Registro delle Imprese	0583976654	
Manca Nicoletta	Registro delle Imprese	0583976420	
Martinelli Stefano	Registro delle Imprese	0583976644	
Meccariello Claudio	Registro delle Imprese	0583976404	
Raffaelli Paola	Registro delle Imprese	0583976650	

COGNOME NOME	UFFICIO COMPETENTE	WORK PHONE	MOBILE
Rizzuti Raffaella	Registro delle Imprese	0583976653	
Sciortinob Mariarosa	Registro delle Imprese	0583976303	
Spinelli Maria Cristina	Registro delle Imprese	0583976302	
Stagi Luca	Registro delle Imprese	0583976608	
Pasquini Marco	Artigianato, Protesti, Documenti Export	0583976601	
Barbieri Nicola	Artigianato, Protesti, Documenti Export	0583976304	
Barsetti Monica	Artigianato, Protesti, Documenti Export	0583976662	
Bianchi Romina	Artigianato, Protesti, Documenti Export	0583976663	
Clemente Maurizio	Artigianato, Protesti, Documenti Export	0583976669	
Giannotti Romana	Artigianato, Protesti, Documenti Export	0583976620	
Luisa Golia Maria	Artigianato, Protesti, Documenti Export	0583976606	
Martini Enrica	Artigianato, Protesti, Documenti Export	0583976605	
Salvetti Olga	Artigianato, Protesti, Documenti Export	0583976672	
Giovannini Morena	Diritto Annuale	0583976685	
Dal Porto Carla	Diritto Annuale	0583976418	
Niccolai Maido	Brevetti e Funzioni ispettive	0583976401	
Della Nina Paolo	Brevetti e Funzioni ispettive	0583976627	
Saraff Alessandro	Brevetti e Funzioni ispettive	0583976635	
Pedone Anna Maria	Arbitrato e Conciliazione	0583976692	
Lotti Enrica	Arbitrato e Conciliazione	0583976645	
Palla Stefano	Arbitrato e Conciliazione	0583976641	
Pedreschi Milena	Arbitrato e Conciliazione	0583976434	
Galli Silvia	Segreteria e Protocollo	0583976655	

COGNOME NOME	UFFICIO COMPETENTE	WORK PHONE	MOBILE
Ferti Francesca	Segreteria e Protocollo	0583976413	
Baldocchi Mauro	Segreteria e Protocollo	0583976668	
Sargenti Francesca	Relazione con l'Esterno	0583976686	
Vecchi Delia	Relazione con l'Esterno	0583976661	

7.4 Team operativo di Disaster Recovery

E' il gruppo di supporto competente per la riattivazione dei servizi informatici.

COGNOME	NOME	UFFICIO COMPETENTE	WORK PHONE	MOBILE
Guidi	Francesco	Provveditorato Funzioni Informatiche	0583976695	

7.5 Ufficio Stampa

E' la funzione deputata alla gestione contatti con la stampa.

COGNOME	NOME	UFFICIO COMPETENTE	WORK PHONE	MOBILE
Sargenti	Francesca	Ufficio Relazioni con l'Esterno	0583976686	
Vecchi	Delia	Ufficio Relazioni con l'Esterno	0583976661	

8. Fornitori

Denominazione : INFOCAMERE SCpA	
Descrizione	Società di Informatica delle Camere di Commercio italiane
Indirizzo	Corso Stati Uniti, 14 – 35127 PADOVA
Telefono	049-8089610
Fornitore di servizi; Infocamere, nel gestire la crisi, procede secondo quanto previsto dai suoi processi di gestione incident, problem management e gestione della crisi, basati su procedure interne Infocamere (procedura MG/107 e suoi allegati), certificate secondo standard ITIL e ISO27001 e documentate nei processi interni Infocamere. Il Piano di Continuità Operativa e il Piano di Disaster Recovery sono gestiti dalla stessa Infocamere.	

Denominazione : LUCENSE S.c.p.A.	
Descrizione	Lucense S.c.p.A
Indirizzo	Via della Chiesa XXXII, trav.I n.231, Sorbano del Giudice 55100 Lucca
Telefono	0583 493616
Sintesi degli accordi contrattuali in essere: **I rapporti e gli aspetti contrattuali con la Società Lucense ScpA, relativamente alla fornitura del servizio in hosting del sito istituzionale www.lu.camcom.it , sono stati curati dall'Ufficio URE con i provvedimenti DD 92 del 18/03/2014 e 42 del 05/02/2015.** **Il servizio è stato aggiudicato ricorrendo al portale MEPA.**	

9. Riferimenti

- **Norma – ISO 22301:2012**

"Societal Security - Business continuity management system - Requirements"

- **Norma ISO/IEC 24762:2008**

"Information technology - Security techniques - Guidelines for information and communication technology disaster recovery continuity"

- **Norma ISO/IEC 27031:2011**

"Information technology - Security techniques - Guidelines for information and communication technology readiness for business continuity"

- **Piano AGID**

Piano AGID_linea guida PCO Piano di Emergenza secondo DL 81/2008

- **Piano di Protezione Civile**

secondo l'Ordinanza del Presidente del Consiglio dei Ministri del 28 agosto 2007, n.3606;

Camera di Commercio di LUCCA

"Continuità operativa" - C.A.D. Art. 50 bis

Piano di Disaster Recovery ICT

Versione Documento	V1.0
Data emissione	_____
Redatto da :	Claudio Mori
Verificato da :	Giunta Camerale
Approvato da :	Delibera di Giunta _____
Autorizzato da :	Dr. Roberto Camisi – Segretario Generale Camera di Commercio di Lucca2014 Dr. Giorgio Bartoli - Presidente Camera di Commercio di Lucca2014

10. INTRODUZIONE 41

10.1 Finalità e contenuti del Piano di Disaster Recovery 41

11. DESCRIZIONE DELLA SOLUZIONE DI DISASTER RECOVERY 42

12. OBIETTIVI DEL PIANO DI DISASTER RECOVERY (PIANO DI DR).....46

13. INFORMAZIONI RELATIVE AL PIANO DI DR.....48

14. CLAUSOLE E DIRETTIVE APPLICABILI 50

15. PERIMETRO DI RIFERIMENTO DEL PIANO 50

15.1 Descrizione del sistema informativo primario e dei servizi critici che la soluzione di DR deve garantire

15.2 Fattori critici e di rischio, descrizione dei casi di disastro/indisponibilità prolungata che si intendono affrontare con la soluzione di DR

15,3 Fattori critici e di rischio: elenco dei possibili rischi

15.4 Sicurezza Informatica

15.5 Descrizione dei casi di disastro/indisponibilità

16. ORGANIZZAZIONE E PERSONALE 59

17. POLITICA DI SICUREZZA E DI SALVAGUARDIA DEI DATI 61

18. FASI DELLA SOLUZIONE DI DISASTER RECOVERY 63

19. PROCEDURE DI TEST.....69

10. INTRODUZIONE

Il sistema informativo di un Ente locale rappresenta il punto cardine per l'attività lavorativa dell'Amministrazione e l'erogazione dei servizi ai cittadini. Il sistema informativo è a sua volta basato su un sistema informatico che, in caso di problema, causerebbe l'interruzione di svariati servizi, causando disservizio agli utenti e di conseguenza ai dipendenti dell'Amministrazione. I danni derivanti da tali interruzioni sono valutabili però anche in funzione del tempo di ripristino dei servizi e di tutto il sistema informatico. Il corretto utilizzo e funzionamento del sistema informatico dell'Ente rappresentano inoltre la base per garantire integrità, disponibilità e riservatezza dei dati trattati, secondo quanto prescritto dal D.
Lgs. 196/2003. Il Piano di Disaster Recovery è l'insieme delle informazioni legate alle azioni, ai sistemi e ai dati con i quali l'Amministrazione Comunale provvede al ripristino delle funzionalità tecnologiche e organizzative della propria struttura.
La predisposizione di un Piano di Disaster Recovery non garantisce all'Ente la continuità dei processi aziendali in caso di disastro in quanto il documento racchiude le informazioni della sola funzionalità del sistema informatico, mentre gli aspetti legati alla gestione delle risorse e all'organizzazione vengono inquadrati all'interno del Piano di Continuità Operativa, di cui il Piano di Disaster Recovery è una parte integrante.

10.1 Finalità e contenuti del Piano di Disaster Recovery

Il Piano di Disaster Recovery, parte integrante del Piano di Continuità Operativa dell'Ente, viene descritto in questa sezione appositamente rubricata ed ha la funzione di spiegare nel dettaglio le fasi necessarie per il ripristino delle risorse hardware e software utilizzate per l'erogazione dei servizi da parte dei dipendenti dell'Amministrazione.
Nel piano di DR vengono dettagliate le procedure operative necessarie per effettuare una corretta valutazione della situazione di emergenza/disastro che non consenta la normale erogazione dei servizi ai cittadini e alle imprese da parte dell'Ente. Nel presente documento vengono inoltre descritte le varie fasi per provvedere al ripristino del sistema informativo primario, ovvero del recupero dei dati e la riconfigurazione delle procedure per arginare e rientrare dallo stato di emergenza dichiarato. Vengono inoltre esposte nel piano di DR le procedure per l'attivazione del sito di DR nel caso non sia accessibile e utilizzabile il sito primario.
L'Ente ha inoltre provveduto all'analisi delle minacce possibili e dei relativi rischi che possono derivare sia da una non corretta gestione dell'infrastruttura informatica, sia dall'integrità delle apparecchiature elettroniche ed informatiche. La sicurezza e l'integrità dei dati, in termini di protezione degli stessi da varie tipologie di cause, esterne ed interne all'Ente, ha permesso di raggiungere livelli di sicurezza che permettano una drastica diminuzione delle probabilità di rischio.
L'integrità fisica dei sistemi informatici, dettagliata nei paragrafi successivi, può infatti essere intaccata o distrutta da calamità naturali (alluvioni, terremoti, fulmini, etc.), da cause accidentali (incidenti, allagamenti, distruzione dell'edificio, distruzione di personal computer, server o altri elaboratori elettronici in cui siano custoditi i dati trattati), da cause esterne (sommosse, rivolte, devastazioni, atti vandalici, eventi socio-politici).
Per assicurare l'integrità fisica dei sistemi informatici si possono inoltre adottare alcuni accorgimenti di minimo costo per proteggere fisicamente i sistemi informatici come ad esempio la collocazione degli elaboratori elettronici non a diretto contatto con il piano di calpestio per evitare o limitare i danni in caso di allagamento oppure al riparo da luoghi di passaggio per evitare rotture accidentali dovute a caduta.
L'integrità fisica delle infrastrutture, dettagliata nei paragrafi successivi, necessaria per il funzionamento dei sistemi e per poter consentire una normale attività lavorativa ai dipendenti dell'Ente, deve essere assicurata dalla continua presenza dell'elettricità nello stabile e della connessione di rete.

Deve inoltre essere prevista la disponibilità di Dispositivi UPS (Gruppi di Continuità), di linee di backup o di emergenza, in grado di subentrare in caso di guasti di varia natura, da attivare con fornitori diversi, se possibile, e nella possibilità tecnica che si attestino su centrali diverse.
Per l'integrità fisica delle infrastrutture è necessario che gli stabili utilizzati risultino, sotto il profilo prevenzionistico, essere conformi alle vigenti disposizioni in materia di igiene e sicurezza sul lavoro (D. Lgs. 81/2008) e di prevenzione incendi (DPR 157/2011 – D.M. 10/03/98).
L'integrità dei dati, indispensabile nell'attività lavorativa di un ente locale, deve sempre essere garantita e potrebbe essere compromessa da semplici errori umani del personale, da guasti dell'hardware, da furto di dati o di credenziali di accesso al sistema, da azioni di hacking.
Per limitare almeno la perdita dei dati o l'alterazione degli stessi è necessario predisporre minimi livelli di sicurezza e garantire un corretto e costante backup dei dati trattati, come nel seguito meglio dettagliato nel paragrafo rubricato "Politiche di sicurezza e salvaguardia dei dati".
La condizione minima e indispensabile per evitare la perdita dei dati trattati è l'esecuzione di corrette copie di backup, conservate e custodite presso un sito alternativo alla Casa Comunale (al sito di produzione dei dati stessi) in cui risulta ubicato il Centro di Elaborazione dei Dati dell'Ente.

L'Ente, dopo l'analisi delle varie tipologie di dati trattati e della spesa da sostenere, ha provveduto a configurare e implementare una soluzione tecnologica di tipo “hosting”, con la quale vengono sincronizzati i dati entro le 24 ore rispetto alla produzione degli stessi.
Tale soluzione può essere garantita in quanto il volume dei dati giornalmente modificati, risulta congruente con la velocità delle n. 2 linee _____ , per una trasmissione giornaliera.
Nel momento in cui vi sarà una produzione di dati superiore, verranno richieste ai provider specifiche di linea adeguate.

11. DESCRIZIONE DELLA SOLUZIONE DI DISASTER RECOVERY

Questa sezione viene dedicata alla descrizione della soluzione di disaster recovery adottata dall’Ente per assicurare la continuità di funzionamento del sistema informatico a fronte di eventi dannosi che comportino un’indisponibilità del servizio oltre la soglia di tolleranza.

Esistono una serie di Programmi e Dati non inseriti nel piano e quindi nel servizio di DR, in quanto già fruibili tramite Internet e quindi disponibili esternamente nel caso di intervento del piano di Disaster.
Tali Programmi sono riportati al capitolo 5. Elenco Servizi voce “Servizi forniti da InfoCamere”.
Inoltre esistono servizi quali IL SITO ISTITUZIONALE anch'esso erogato da fornitore esterno all'Ente.
Per tali casistiche si rimanda ai piani di DR delle specifiche aziende fornitrici dei servizi.

Esistono inoltre Servizi erogati direttamente dalla Camera di Commercio di Lucca ed interni al CED quali:

Classe di Servizi : PRESENZE DEL PERSONALE		
Rilevazione delle presenze del personale camerale		
servizi componenti : – Rilevazione presenze del personale camerale	Fornitore :	**Camera di Commercio di Lucca**
	Tipologia utente :	Interno
	Indice complessivo di criticità :	3
	Classe di criticità :	media
	Soluzione tecnologica :	TIER 2
	RPO :	24 ore
	RTO :	72 ore

a questi vanno aggiunti servizi quali l'authentication Server, File server, ed altre servizi legati al corretto funzionamento ed alla produttività delle postazioni fisiche che in caso di Disaster devono essere ripristinati nel tempo più breve possibile..
La Camera di Commercio di Lucca ha previsto, come soluzione di Disaster Recovery, la costituzione di un servizio in hosting con InfoCamere SCPA per la replica dei Server con funzioni di:

- Domain controller
- File Server
- Print Server

Il processo decisionale dell'Ente ha tenuto conto dei seguenti elementi:

- le caratteristiche della rete camerale;
- le caratteristiche dei collegamenti tra il sito primario ed il secondario, in termini di capacità di trasmissione, di disponibilità, di ridondanza e possibilità di collegamenti alternativi, ponendo attenzione in merito a come tali caratteristiche permettano di soddisfare in maniera totale o parziale le esigenze del servizio;
- le modalità di recupero dei dati e di verifica della loro consistenza e completezza;
- se e come il servizio erogato dal sito secondario abbia le stesse caratteristiche di quello primario;

rete camerale - ICRete
Il sistema camerale è dotato di una rete di trasmissione dati geografica nazionale che collega tutte le Camere di Commercio. Tale rete, denominata nel seguito ICRete (InfoCamere Rete), ha lo scopo di supportare un sistema informatico nazionale in grado di trattare e distribuire in tempo reale atti e documenti che la legge dispone siano oggetto di pubblicità legale o di pubblicità notizia o che comunque scaturiscano da registri, albi, ruoli, elenchi e repertori tenuti dalle Camere di Commercio stesse.
L'architettura della rete è stata realizzata ed è attualmente gestita da InfoCamere (società consortile delle Camere di Commercio) per rispondere alla duplice esigenza di archiviazione e ricerca dei dati mediante la costituzione di un archivio centrale, adeguatamente protetto e ridondato, che consenta di effettuare in modo efficiente e tempestivo la consultazione da qualsiasi punto del territorio nazionale

ICRete contiene oltre 10.000 tra workstation e server, distribuite nelle diverse sedi Camerali centrali e periferiche.

architettura data center InfoCamere
InfoCamere garantisce l'operatività delle Camere di Commercio attraverso un Data Center evoluto, basato su ambienti open, che adotta le migliori tecnologie oggi presenti sul mercato in ambito di virtualizzazione, di sistemi hardware, di sistemi storage, di sistemi di controllo, di software.
L'architettura della rete è stata realizzata da InfoCamere per rispondere all'esigenza di archiviazione e ricerca dei dati su scala nazionale, mediante la costituzione di un archivio centrale che consente di effettuare in modo efficiente e tempestivo la consultazione da qualsiasi punto del territorio. Attualmente i servizi forniti dal sistema informatico nazionale sono erogati da un insieme di server ospitati presso le sedi dei Data Center InfoCamere di Padova e Milano. Presso il centro di produzione di Padova, un sistema di monitoraggio controlla istante per istante l'efficienza del servizio, rileva il verificarsi di inconvenienti tramite opportuni strumenti diagnostici, attiva i necessari interventi specialistici e fornisce un supporto operativo on line. InfoCamere deve garantire livelli elevati di servizio e di sicurezza dei dati nell'ambito dell'architettura di rete. Per

questo motivo InfoCamere ha costituito una rete nazionale, denominata ICRete, che si basa su due distinte infrastrutture di rete in tecnologia MPLS costituita attualmente da due dorsali di rete, denominate A e B. Queste due piattaforme sono di due Operatori distinti e pertanto completamente separate

caratteristiche dei collegamenti
Le dorsali A e B di ICRete, realizzate in tecnologia MPLS, collegano ai Data Center InfoCamere di Padova e Milano e sono rispettivamente fornite da Fastweb e da TIM:

- tutte le sedi principali delle Camere di Commercio
- alcune sedi secondarie delle Camere di Commercio
- le società del gruppo InfoCamere
- altri Enti del Sistema Camerale

Le caratteristiche principali di ICRete sono:

- accessi alle dorsali A e B in GigabitEthernet presso i Data Center InfoCamere di Padova e Milano
- link di connessione diretta tra i Data Center di Padova e Milano costituita da 2 flussi GigabitEthernet
- instradamento del traffico immediato e automatico, in caso di interruzione di un link di una Dorsale
- tempi di risposta di rete costanti e controllati
- alta disponibilità (99,99 %)
- centro di controllo sempre attivo
- gestione guasti di rete centralizzata
- livelli di servizio definiti e controlla

InfoCamere dispone di sistemi di sicurezza, quali firewall, antivirus, antiSPAM, IPS. La maggior parte delle informazioni di sicurezza (log) prodotte da questi sistemi sono raccolte in un sistema di controllo (SIEM) basato sul prodotto Splunk. Vi afferiscono in particolare i log dei sistemi Checkpoint e dell'IPS TippingPoint.

Le fonti su cui InfoCamere propone il prelievo sono:
• SIEM su tecnologia Splunk
• Bilanciatore F5, con decodifica/ricodifica del traffico HTTPS
• Firewall Checkpoint, con accesso mediate API proprietarie (OPSEC)

<u>Periodicamente InfoCamere commissiona a terzi analisi di sicurezza infrastrutturale ed applicativa.</u>

La soluzione proposta da InfoCamere
In considerazione di quanto richiesto dalla CCIAA, InfoCamere propone l'adozione di un servizio di Hosting remoto replicato – HRR.

Questo servizio consente di centralizzare e replicare servizi specifici quali :

- Servizi di Active Directory (autenticazione, dominio centrale, policy di lavoro, etc)
- DNS e DHCP
- Servizi di file server
- Servizi di Print Server,

in modo da adempiere alle normative CAD (Codice di Amministrazione Digitale) secondo quanto previsto dall'art. 50 bis, e costituisce un mattone fondamentale per la *Continuous Availability* e la *Disaster Recovery* previste dalla normativa.

Principali Benefici della Soluzione

I benefici della soluzione proposta sono di seguito riepilogati :

- maggiore sicurezza, aderenza ai requisiti previsti da Digit PA;
- maggiore affidabilità e continuità dei servizi, essendo ospitati in DataCenter evoluto (Standard TIA 942) con presidio costante di personale professionale;
- maggiore flessibilità e scalabilità : a fronte di nuove esigenze, sarà possibile accedere più facilmente e velocemente a risorse aggiuntive previa valutazione economica del cliente dei nuovi impegni;
- minori costi per l'attivazione di ulteriori servizi di Disaster Recovery essendo facilmente utilizzabile i DataCenter di DR di InfoCamere (da valutare dopo la conclusione completa delle attività).

Inoltre il complesso di tali servizi consentirà, nel tempo, concreti risparmi economici in termini di:

- minori fabbisogni energetici e spazi dedicati localmente a CED;
- minori investimenti legati a possibili adeguamenti inerenti la sicurezza fisica dei CED locali;
- minori investimenti in termini di manutenzione ed aggiornamento dell'hardware e dei software;
- minor impegno di risorse locali dedicate al funzionamento dell'intera infrastruttura.

Descrizione del servizio HRR

La soluzione prevede la predisposizione di uno o più server virtuali, normalmente presso il DataCenter di Padova con il ruolo di:

- Controller primario del dominio con autenticazione degli utenti/postazioni;
- DNS, DHCP, WSUS Server;
- File Server (repository file);
- Print Server (a richiesta)

InfoCamere, sfruttando la propria rete ed il Datacenter, **replicherà** i dati ed i servizi suddetti attraverso nuove macchine virtuali appositamente predisposte. Tali sistemi avranno gli stessi ruoli, svolgeranno le medesime funzioni delle macchine originali presenti in CCIAA. In questo modo otterremo server speculari ma siti in locazioni diverse, coerentemente con l'esigenza di garantire la "*Continuità Operativa"* su tali servizi.

L'accesso "Primario" delle postazioni di lavoro del cliente, sia fisiche che eventualmente virtuali, avverrà attraverso l'infrastruttura predisposta in CCIAA di Lucca.
Qualora i server locali non fossero accessibili, tutte le postazioni di lavoro si attesteranno automaticamente e trasparentemente sui server posizionati nel Datacenter di Padova.
In particolare, il servizio di File Server sarà replicato mediante la funzionalità di Distribution File Server Replicated (DFS-R).

La soluzione tecnica adottata, rappresentata sostanzialmente da una replica dei Server centrale nella macchina Virtuale della sede di DR, consente, in caso di avaria hardware o software delle unità elaborative della Camera di Commercio di Lucca, di attivare in tempi ridottissimi le funzionalità replicate sul sito remoto. In caso di necessità, grazie ad una corretta pianificazione delle modalità e dei tempi di ripristino, sarà infatti possibile rendere produttiva la Macchina Virtuale nel sito di DR e garantire l'attività lavorativa dei principali uffici dell'Ente, a vantaggio degli utenti finali.

L'unica criticità alla soluzione di DR è rappresentata dall'indisponibilità del collegamento all'interno della rete geografica ICrete.
Infatti in caso di avaria di uno qualsiasi dei componenti della catena di rete che va dagli apparati di rete attivi (switch), dai router e dalla connettività potrebbe portare ad una mancanza di utilizzo delle risorse elaborative disponibili sul sito di DR. Questa è sicuramente una "criticità" conosciuta e ovvia data dalle seguenti soluzioni:

connettività
Le dorsali A e B di ICRete, realizzate in tecnologia MPLS, collegano il sistema camerale ai Data Center InfoCamere di Padova e Milano e sono rispettivamente fornite da Fastweb e da TIM.
Pertanto la mancanza di connettività da parte di uno dei gestori sopra indicati verrà sostituita dall'altro.

apparati attivi
in caso di eventi che provochino la distruzione o il danneggiamento degli apparati attivi e dei router, Infocamere provvederà, a seguito di un contratto di manutenzione e assisetnza degli stessi, a sostituire entro 48 ore le apparecchiature.

12. OBIETTIVI DEL PIANO DI DISASTER RECOVERY (PIANO DI DR)

Obiettivo principale del piano di DR deve essere quello di pianificare tutte le attività di gestione e manutenzione della soluzione di DR in caso di normale svolgimento dell'attività lavorativa e di assicurare
in condizioni di emergenza l'attuazione delle corrette procedure per il ripristino del sistema e il rientro
dall'emergenza, con conseguente ripresa dell'erogazione dei servizi.
Il Piano di Disaster Recovery rappresenta l'insieme delle misure tecnologiche e organizzative necessarie
per poter provvedere al ripristino del sistema informatico e dei dati dell'Ente in modo da riattivare l'erogazione dei servizi.
Nel caso in cui l'Ente non abbia a disposizione elaboratori elettronici pronti all'utilizzo nell'eventualità di
un'emergenza, ci dovrà essere un fornitore esterno con cui l'Ente ha predisposto apposito contratto, che
garantisce tempi di intervento ben definiti e prestabiliti, renderà disponibili personal computer e altre
apparecchiature necessarie per permettere una riattivazione dei servizi.

Nello specifico sarà necessario che l'Ente, attraverso le figure dei fornitori dei gestionali e dell'amministratore di sistema, prenda i dati salvati e custoditi nel sito remoto e provveda a ripristinare su un elaboratore elettronico i software gestionali e le banche dati. Una volta provveduto a questo primo ripristino sarà necessario verificare la correttezza dei dati recuperati e configurare i pc, già nelle disponibilità dell'Ente. Questi pc saranno utilizzati dai dipendenti per proseguire nell'erogazione dei servizi, ovvero riattivare l'erogazione degli stessi in caso di emergenza.

I servizi per i quali sarà necessario un immediato ripristino sono di seguito elencati:

Servizio / Classe di Servizi	Indice complessivo di criticità	Classe di criticità	Soluzione tecnologica (Tier)	RPO da autovalutazione	RTO da autovalutazione
Altri registri albi e ruoli [Italiancom]	4	Media	2	1 giorno	3 giorni
Archivio PARD e Albi Camerali	5	Media	4	4 ore	3 giorni
Carte Tachigrafiche	5	Media	3	1 giorno	3 giorni
Contabilità, Pianificazione, Controllo di Gestione ed Amministrazione Aperta	5	Media	3	1 giorno	3 giorni
Diritto Annuale	5	Media	3	1 giorno	3 giorni
Facilitazione Gestione Attività Camerali	4	Media	2	1 giorno	3 giorni
Marchi e Brevetti	5	Media	3	1 giorno	3 giorni
Registro Imprese	5	Media	4	4 ore	3 giorni
Registro informatico dei Protesti	5	Media	3	1 giorno	3 giorni
Rete Telematica e Servizi di Connettività [Internet, Posta Elettronica]	6	Alta	4	1 ora	3 giorni
Sanzioni Amministrative	5	Media	3	1 giorno	3 giorni
Servizi di Conciliazione ed Arbitrato	5	Media	3	1 giorno	3 giorni
Servizi di Gestione Documentale	5	Media	4	4 ore	3 giorni
Servizi per l'Ambiente	4	Media	3	1 giorno	3 giorni
Vigilanza e Controllo Prodotti, Metrologia Legale	4	Media	2	1 giorno	3 giorni
Certificati di origine merci [Cert'O]	4	Media	4	1 giorno	3 giorni
Presenze del Personale	3	Media	2	1 giorno	3 giorni
Sito istituzionale	3	Media	2	1 giorno	3 giorni

Si ricorda inoltre che tutti i servizi sopra elencati, ad eccezione di **Presenze del Personale ,** sono in Hosting, o gestiti da differenti ditte per cui risiedono presso i Data Center delle aziende fornitrici dei servizi, e garantiscono tempi di ripristino immediati dei servizi presenti nelle loro piattaforme in quanto vengono riversati anche su altri data center di backup, provvedendo loro stessi ai propri piani di DR.

13. INFORMAZIONI RELATIVE AL PIANO DI DR

Informazioni Statiche e Informazioni Dinamiche

Informazioni Statiche: informazioni che rimarranno costanti e non saranno oggetto di frequente revisione.
Rientrano in questa sezione tutte le informazioni strutturali relative agli stabili che ospitano sia la sede principale ,c.te campana 10 – 55100 Lucca, che la sede secondaria, Via Leònida Rèpaci, 16 – 55049 Viareggio.
Si precisa che il sito primario risulta, sotto il profilo prevenzionistico, essere conforme alle vigenti disposizioni in materia di igiene e sicurezza sul lavoro (D. Lgs. 81/2008) e di prevenzione incendi (DPR
157/2011 – D.M. 10/03/98).

Alimentazione Elettrica. Le sedi della Camera di Commercio di Lucca sono dotate di impianto elettrico cablato a norma di legge.
I server di rete, gli apparati di rete sono protetti da gruppi di continuità UPS atti a garantire la necessaria protezione delle apparecchiature informatiche dagli sbalzi e dall'interruzione della corrente elettrica di rete, fornendo il tempo necessario al corretto spegnimento dei sistemi informatici ad essi collegati.

Sistemi antincendio. Le sedi sono provviste di estintori portatili a polvere e CO2, regolarmente manutenuti. In prossimità degli ambienti CED sono presenti estintori portatili a polvere e co2.

Sistemi antintrusione. Risulta inoltre attivo un sistema anti intrusione, dotato di allarme sonoro con sensori volumetrici ubicati nelle parti comuni degli edifici.

Aree di emergenza. Non sono presenti locali attrezzati in caso di parziale inagibilità degli uffici comunali, ma grazie all'interoperabilità delle postazioni di lavoro è possibile riallocare i dipendenti negli
uffici ancora agibili.

Accesso alle banche dati e internet. L'Ente è dotato di sistema di autenticazione informatica al proprio sistema informativo, come previsto dal D. Lgs. 196/2003 e succ., automatizzato tramite funzionalità Active Directory di Windows oltre a software antivirus, presente su tutti i client, firewall su hardware dedicato con Antivirus, Antispam e Context Filtering. La connessione ad internet viene
fornita da InfoCamere SCPA (società consortile delle Camere di Commercio). Gli edifici sono dotati di cablaggio di rete strutturato su cavi in rame UTP di categoria 5E.

La CCIAA ha il seguente organigramma :

Nome Servizio	Ufficio Competente	Nome Responsabile Ufficio
Area SEGRETERIA GENERALE / ORGANI	Programmazione e Controllo	Dr.ssa Gabriella De Blasio
Area SEGRETERIA GENERALE / ORGANI	Segreteria e Protocollo	Dr.ssa Silvia Galli
Area SEGRETERIA GENERALE / ORGANI	Ufficio Personale	Dr.ssa Serena Marchetti
Servizio Anagrafico Certificativa, Studi, Politiche Economiche e Regolazione di Mercato	Registro Imprese Artigianato, Protesti, Documenti Export	Dr.ssa Alessandra Nardone
Servizio Anagrafico Certificativa, Studi, Politiche Economiche e Regolazione di Mercato	Registro Imprese	Dr.ssa Manuela Salani
Servizio Anagrafico Certificativa, Studi, Politiche Economiche e Regolazione di Mercato	Artigianato, Protesti, Documenti Export	Dr. Marco Pasquini
Servizio Anagrafico Certificativa, Studi, Politiche Economiche e Regolazione di Mercato	Ufficio Sede Distaccata di Viareggio	
Servizio, Studi, Politiche Economiche e Regolazione di Mercato	Segreteria e Protocollo Studi e Statistica Politiche Economiche e Infrastrutture Relazioni con l.Esterno	Dr.ssa Giovannella Brandani
Servizio, Studi, Politiche Economiche e Regolazione di Mercato	Ufficio Arbitrato e Conciliazione	Dr.ssa Anna Maria Pedone
Servizio, Studi, Politiche Economiche e Regolazione di MercatoServizio, Studi, Politiche Economiche e Regolazione di Mercato	Ufficio Brevetti e Funzioni Ispettive	Dr. Maido Niccolai
Servizio, Studi, Politiche Economiche e Regolazione di Mercato	Studi e Statistica	Dr. Massimo Pazzarelli
Servizio, Studi, Politiche Economiche e Regolazione di Mercato	Politiche Economiche e Infrastrutture	Dr.ssa Alisa Maionchi
DIRIGENTE AREA PROMOZIONE E SVILUPPO PER LE IMPRESE, AMMINISTRAZIONE	Relazioni Esterne	Dr.ssa Francesca Sargenti
Servizio Promozione e Sviluppo per le Imprese	Promozione Interna ed Estera Sviluppo Imprenditoriale Brevetti Marchi e Innovazione Tecnologica	Dr.ssa Marta Piacente
Servizio Promozione e Sviluppo per le Imprese	Promozione Interna ed Estera	Rag. Aurelio Pesci
Servizio Promozione e Sviluppo per le Imprese	Sviluppo Imprenditoriale	Dr.ssa Federica Ramacciotti
Servizio Promozione e Sviluppo per le Imprese	Ufficio Politiche Comunitarie Eurosportello	Sig. Giuseppe Acquaviva
Servizio Gestione Patrimoniale e Finanziaria	Ragioneria Provveditorato Diritto Annuale	Dr.ssa Paola Petroni
Servizio Gestione Patrimoniale e Finanziaria	Ragioneria	Rag. Daniela Rossi
Servizio Gestione Patrimoniale e Finanziaria	Provveditorato	Rag. Luca Granucci
Servizio Gestione Patrimoniale e Finanziaria	Diritto Annuale	Rag. Morena Giovannini

Informazioni Dinamiche: informazioni relative al piano di DR che necessitano di un regolare e costante aggiornamento per provvedere al corretto mantenimento dello stesso piano relativamente

ai cambiamenti che possono essere attuati nell'organizzazione tecnico-operativa dell'Ente. Nello specifico sono elencate in apposito inventario (costantemente aggiornato) tutte le apparecchiature del sistema informatico e informativo dell'Ente, oltre che gli eventuali aggiornamenti ovvero nuove acquisizioni di elaboratori elettronici o altro materiale HW e SW, compresi quelli utilizzati per la soluzione di DR.
Gli argomenti di seguito trattati fanno parte delle informazioni dinamiche per cui l'Ente potrebbe provvedere all'aggiornamento nel corso dei prossimi esercizi.

Backup. Le procedure di custodia dei dati trattati dall'ente prevedono l'impiego di soluzioni che contemplano sia il Backup locale secondo la normativa sulla privacy (già descritto precedentemente), sia
la replica, sulle macchine virtuali del sito DR, dei dati e programmi presenti sulle unità elaborative del
Server, garantendo così disponibilità dei dati e funzionalità del sito di DR.

Sistemi di protezione dati sugli elaboratori centrali. Sui sistemi informatici dell'Ente identificati come critici, sono presenti i seguenti sistemi di protezione:
· Server Dati: Doppio Hard Disk in configurazione Mirroring (RAID 1).
· Server NAS: Doppio Hard Disk da 1TByte in configurazione Mirroring (RAID 1)
Nell'eventualità di evento disastroso che interessi unicamente l'unità elaborativa Server, sarà necessario
commutare l'attività lavorativa sul sito di DR, continuando al lavorare tramite Desktop Remoto.

Contratti di assistenza tecnica. Sono attivi i contratti di assistenza manutenzione di servizi per le procedure gestionali informatizzate dell'Ente fornite da:
InfoCamere SCPA
Lucense SCPA

Per quanto concerne l'assistenza sistemistica è prevista solo quella per i server principali, acquistia tramite MEPA Mercato Elettronico della Pubblica Amministrazione.

14. CLAUSOLE E DIRETTIVE APPLICABILI

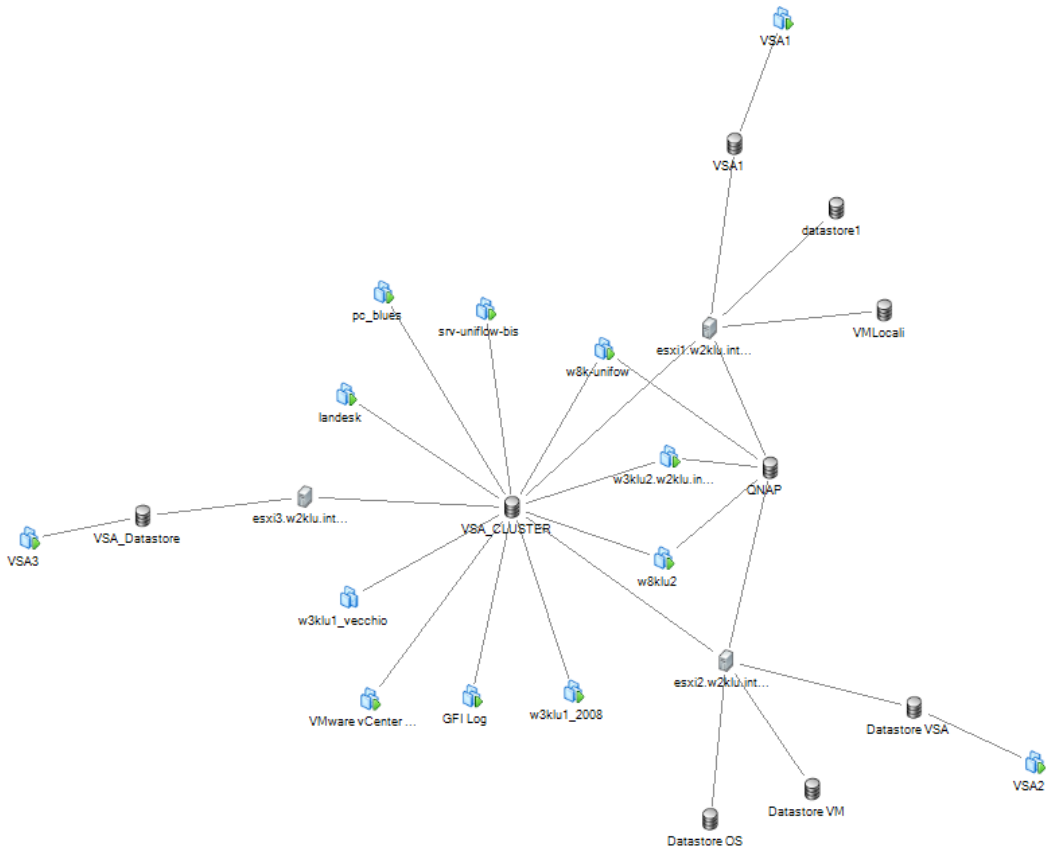
Norme e riferimenti di standard a cui deve fare riferimento il Piano di DR:
Documento Programmatico sulla Sicurezza per la protezione dei dati personali;
Codice dell'Amministrazione Digitale D. Lgs. 82/2005;
Nuovo Codice dell'Amministrazione Digitale D. Lgs. 235/2010;
Circolare 1 dicembre 2011 n. 58 "Attività di DigitPA e delle Amministrazioni ai fini dell'attuazione degli
adempimenti previsti dall'articolo 50 -bis (Continuità Operativa) del «Codice dell'Amministrazione
Digitale» (D.lgs. n. 82/2005 così come modificato dal D.lgs. 235/2010)";
Linee guida per il Disaster Recovery delle Pubbliche Amministrazioni, ai sensi del comma 3, lettera
b)dell'art. 50-bis del D. Lgs. n. 82/2005 e s.m.i..

15. PERIMETRO DI RIFERIMENTO DEL PIANO

15.1 Descrizione del sistema informativo primario che la soluzione di DR deve garantire

L'Ente possiede una propria struttura informatica, internamente agli edifici sulla rete locale LAN, strutturata secondo il sistema informativo basato sul modello **Client/Server**.
Le apparecchiature principali per l'elaborazione e la salvaguardia dei dati, assieme agli apparati intermedi
di rete attivi e passivi, sono posizionati al III piano dell'edificio di corte Campana, 10, in un armadio costruito ad Hoc all'interno del locale CED

SCHEMA DELLA STRUTTURA INFORMATICA



Tipologia e caratteristiche dei server ospitanti la virtualizzazione

Numero 3 nodi:

esx1.w2klu.cciaa.net

Manufacturer:	HP
Model:	ProLiant DL385 G5p

Processors:	8 CPU x 2,7 GHz
Processor Type:	Quad-Core AMD Opteron(tm) Processor 2384
Hyperthreading:	Inactive
Total Memory:	40,00 GB
Number of NICs:	6
State:	Connected
Virtual Machines:	4
vMotion Enabled:	Yes
Active Tasks:	No

esx2.w2klu.cciaa.net

Manufacturer:	HP
Model:	ProLiant DL385 G6
Processors:	12 CPU x 2,6 GHz
Processor Type:	Six-Core AMD Opteron(tm) Processor 2435
Hyperthreading:	Inactive
Total Memory:	32,00 GB
Number of NICs:	8
State:	Connected
Virtual Machines:	4
vMotion Enabled:	Yes
Active Tasks:	No

esx3.w2klu.cciaa.net

Manufacturer:	HP

Model:	ProLiant DL385p Gen8
Processors:	24 CPU x 2,593 GHz
Processor Type:	AMD Opteron(tm) Processor 6344
Hyperthreading:	Inactive
Total Memory:	31,95 GB
Number of NICs:	6
State:	Connected
Virtual Machines:	5
vMotion Enabled:	Yes
Active Tasks:	No

tipologia e versione del virtualizzatore

vCenter Server 5 Essentials
Vmware vSphere 5 Essentials Plus

15.2 Fattori critici e di rischio, descrizione dei casi di disastro/indisponibilità prolungata che si intendono affrontare con la soluzione di DR

15*.2.1 Fattori critici e di rischio: elenco dei possibili rischi*

In questa sezione vengono dettagliati i rischi possibili e probabili a cui possono essere sottoposte le infrastrutture, fisiche e tecnologiche dell'Ente, e i dati trattati.
Per i dati trattati devono essere garantite le qualità fondamentali che, per espressa previsione normativa,
dati personali oggetto di trattamento debbono sempre possedere e cioè:

a) la **disponibilità,** che assicura che l'accesso ai dati sia disponibile quando necessario. Per garantire
questa "qualità" è necessario che l'accesso alle informazioni o alle risorse informatiche sia negato senza
autorizzazione;

b) l'**integrità,** che garantisce della accuratezza e della completezza dei dati e delle informazioni custodite e contenute all'interno degli elaboratori ovvero sui supporti magnetici o ottici utilizzati per il salvataggio dei dati.

Per garantire questa "qualità" si rende necessario codificare ed adottare delle corrette procedure per il
backup dei dati e nel contempo evitare che le informazioni correttamente salvate possano formare oggetto di modifica o di accesso senza autorizzazione;

c) la **riservatezza,** che garantisce che i dati e le informazioni siano conosciute ed accessibili solo ed
esclusivamente al personale autorizzato. Il rispetto della citata "qualità" si ottiene negando l'accesso alle
informazioni a tutti i soggetti, interni ovvero esterni all'Amministrazione, che non siano legittimati al
trattamento ed alla conoscenza degli stessi dati da una espressa previsione normativa oppure da necessità legate all' espletamento di funzioni istituzionali.

Per garantire il rispetto di queste qualità è necessario conoscere ed analizzare le minacce che potrebbero
incidere sulle stesse.

Per un soggetto Pubblico come l'a Camera di Commercio di Lucca, i danni che possono essere provocati alle Banche Dati che contengono informazioni personali, sensibili o giudiziarie, si possono distinguere in due macro – categorie:

· **DANNI RICOLLEGABILI AD ATTIVITÀ UMANE**
· **DANNI DERIVANTI DA EVENTI NATURALI, INCIDENTI, GUASTI MECCANICI.**

I danni che una persona, autorizzata/legittimata o meno al trattamento può apportare, volutamente inconsciamente, alle banche dati si possono classificare nelle seguenti ipotesi:
· Accesso non autorizzato ad informazioni;
· Modifica non controllata del contenuto delle Banche Dati con conseguente perdita delle caratteristiche di **correttezza, completezza e congruità logica** dei dati stessi;
· Distruzione di Banche Dati;
· Copia non autorizzata dei dati contenuti nelle Banche Dati;
· Malfunzionamento del Servizio;
· Interruzione del Servizio;

Esistono però altri fattori di rischio non legati ad attività umane ma derivanti da eventi naturali, incidenti, avarie, guasti meccanici, che possono comunque determinare malfunzionamenti o, nei
casi più gravi, interruzione di servizi, di cui è necessario tenere conto nella presente analisi.

ANALISI DI DETTAGLIO DEGLI EVENTI CHE POSSONO GENERARE DANNI E CHE COMPORTANO QUINDI RISCHI PER LA SICUREZZA DEI DATI PERSONALI TRATTATI

Gli eventi in grado di determinare dei danni e, conseguentemente, in grado di rappresentare un rischio per la sicurezza dei dati personali trattati dall'Ente, possono essere ricondotti a 3 MACRO-CATEGORIE:

A. EVENTI RICONDUCIBILI AL COMPORTAMENTO UMANO

B. EVENTI RICONDUCIBILI AGLI STRUMENTI INFORMATICI

C. EVENTI RICONDUCIBILI AL CONTESTO FISICO-AMBIENTALE-INFRASTRUTTURALE

Il dettaglio delle minacce e dei rischi propri di ciascuna categoria di EVENTI appare essere il seguente:

A. EVENTI RICONDUCIBILI AL COMPORTAMENTO UMANO

A.01 Accesso non autorizzato ai dati personali trattati mediante impersonamento informatico

La concreta possibilità che si verifichi un'ipotesi di accesso non autorizzato a dati personali trattati su supporto informatico mediante il c.d. "impersonamento informatico" si può avere nelle seguenti situazioni:

I. distrazione ovvero negligenza di un Incaricato del trattamento dei dati il quale, per esempio, lascia incustodita la propria postazione di lavoro collegata ovvero non custodisce diligentemente le proprie credenziali di autenticazione.

II. scambio delle Password tra gli Incaricati.

III. carenza nel sistema e nelle procedure di attribuzione e gestione dei profili di autenticazione e di autorizzazione degli utenti.

Nelle ipotesi di accesso non autorizzato ai dati personali trattati dall'Ente mediante impersonamento informatico, un soggetto non autorizzato (interno ovvero esterno all'Amministrazione stessa), può accedere ai dati, con le credenziali di autenticazione attribuite all'incaricato legittimato all'accesso sostituendosi in tutto e per tutto al soggetto titolare delle stesse.

Secondo quanto espressamente previsto dal D. Lgs. 196/03, ogni dipendente individuato quale Incaricato del trattamento dei dati deve poter accedere **esclusivamente** a quelle informazioni che risultino essere necessarie, pertinenti e non eccedenti per svolgere correttamente il proprio lavoro e porre in essere l'attività istituzionale propria dell'Ufficio.

E' dunque necessario verificare e assicurare che l'accesso ai dati personali, sensibili e giudiziari sia rigorosamente controllato e avvenga esclusivamente ad opera dei soggetti espressamente autorizzati. L'accesso non autorizzato ai dati personali trattati dall'Ente espone agli ulteriori rischi di modifica non autorizzata, di danneggiamento, di mancanza di congruità, di perdita e di esportazione illegittima dei dati stessi.

In riferimento al punto (III.) la Camera di Commercio di Lucca, come già espresso, ha preso tutte le misure di sicurezza creando un Dominio Active Directory con una struttura di password complessa (lettere e numeri) e gruppi di utenza per l'abilitazione alle singole aree informatiche di competenza.

A.02 Insufficiente conoscenza del sistema informatico o dell'applicazione

In alcuni casi, il dipendente individuato quale Incaricato del trattamento dei dati, può involontariamente compiere azioni che comportano un danno semplicemente perché non è perfettamente a conoscenza delle conseguenze del suo operato a causa di una mediocre conoscenza del sistema, dello strumento informatico ovvero dell'applicazione.

Il danno che può essere provocato varia a seconda del comportamento posto in essere e può determinare:

i. Un blocco momentaneo della stazione di lavoro

ii. Un blocco che può coinvolgere anche altri utenti della Rete

iii. L'inserimento, la modifica o la cancellazione (e dunque la perdita) non voluta di informazioni e dati

iv. L'invio di dati personali, sensibili o giudiziari a soggetti non autorizzati

v. La visione di dati personali, sensibili o giudiziari a soggetti non autorizzati

A.03 Insufficiente conoscenza dei rischi e delle misure di sicurezza

Si osserva talvolta negli Incaricati del trattamento dei dati, una sorta di superficialità di comportamento con riferimento alle problematiche relative alla sicurezza informatica. Superficialità dovuta, in genere, ad una non puntuale conoscenza dei gravi rischi che possono determinarsi quale conseguenza di una condotta non improntata al rispetto delle norme tecniche dettate dal D. Lgs. 196/03.

I comportamenti più ricorrenti che si possono ascrivere a questa categoria sono:

i. La diffusione nell'ambito dell'Ufficio, tra colleghi, della componente riservata della credenziale di autenticazione o PASSWORD

ii. La negligente custodia delle credenziali di autenticazione da parte del singolo Incaricato del trattamento

iii. La circostanza che venga lasciata la propria stazione di lavoro accesa e collegata quando ci si assenta per qualsivoglia ragione dall'Ufficio

iv. La circostanza che vengano lasciate, liberamente fruibili, stampe e tabulati contenenti dati personali, sensibili o giudiziari.

Il danno che può essere determinato nelle ipotesi considerate è quello di accesso non autorizzato ai dati personali trattati, di modifica dei dati, di esportazione illegittima degli stessi e, nei casi più gravi, di distruzione.

A.04 Distrazione e Negligenza

La distrazione e la negligenza possono essere di tipo "fisico" ovvero "logico".
La distrazione/negligenza di tipo fisico, in genere, comporta direttamente danni alla strumentazione ed alle attrezzature e, in alcuni casi, indirettamente e conseguentemente danni ai dati (si rovescia la bottiglia dell'acqua sull'unità centrale, si urta la postazione di lavoro facendola cadere e danneggiandola).
La distrazione/negligenza di tipo logico invece, determina in genere esclusivamente danni ai dati trattati (durante la sessione di lavoro l'Incaricato del trattamento viene distratto da una telefonata e dimentica di salvare il documento su cui stava lavorando ovvero preme inavvertitamente dei tasti che provocano l'esecuzione di un comando non voluto).
Il danno che tale evento può determinare sui dati personali oggetto di trattamento è quello di alterazione, corruzione, cancellazione e, nei casi più gravi, perdita dei dati stessi.

A.05 Atto doloso

E' senza dubbio il più grave e pericoloso degli eventi dannosi legati al fattore umano in grado di determinare un danno ai dati personali in quanto presuppone una precisa volontà indirizzata alla manomissione ovvero alla distruzione delle strumentazioni o dei dati trattati.
Potrebbe verificarsi che, con comportamento consapevole, derivante potenzialmente da vari fattori (risentimento verso l'Ente ovvero perseguimento di fini personali), gli Incaricati del trattamento compiano operazioni illecite sulle Banche Dati assegnate.

B. EVENTI RICONDUCIBILI AGLI STRUMENTI INFORMATICI

B.01 Azione di Virus Informatici ovvero di programmi suscettibili di recare danno

Ci si riferisce all'azione di virus informatici programmati per cancellare i dati a cui gli interessati hanno accesso o comunque per danneggiarli, ovvero per causare la paralisi dei servizi erogati mediante gli strumenti informatici.
L'azione di questi agenti dannosi è generalmente innescata dallo scaricamento di programmi eseguibili di varia natura che vengono diffusi per posta elettronica sotto forma di allegati, oppure provengono da siti che, ingannando l'utente, lo inducono a salvare questi file sulla propria postazione di lavoro.

In merito a tale minaccia la Camera di Commercio di Lucca ha impostato:
doppio sistema di antivirus, cioè:

- Antivirus su ogni client
- Filtro Antivirus gestito da Firewall centrale
- Filtro Antispam implementato sul Firewall centrale
- "Filtri Web" all'interno del Firewall centrale per bloccare navigazione su siti pericolosi e/o non etici

B.02 Spamming o tecniche di sabotaggio

Ci si riferisce ad azioni di sabotaggio compiute da terzi tramite programmi che, sfruttando difetti del software utilizzato per la gestione della posta elettronica o di altri servizi informatici, saturano il servizio di richieste fino alla paralisi parziale o totale dello stesso. Questa azione determina l'indisponibilità temporanea dei dati gestiti dal servizio che forma oggetto di attacco.

In merito a tale minaccia la Camera di Commercio di Lucca ha impostato un Filtro Antispam implementato sul Firewall centrale.

B.03 Obsolescenza degli strumenti Hardware

L'obsolescenza delle attrezzature, che nel campo informatico è particolarmente rapida, oltre a rappresentare un fattore di rischio "attivo", può impedire l'attivazione e l'implementazione di misure di sicurezza fisiche o logiche che si rendano opportune per eliminare o ridurre alcuni rischi.

L'esempio che può essere fatto è quello che si riferisce alla impossibilità tecnica di installare su un vecchio elaboratore un sistema di cifratura dei dati che richiede processori di una certa potenza e sufficiente memoria.

In merito a tale obsolescenza, la Camera di Commercio di Lucca ha redatto un Piano Informatico di sviluppo a medio termine coerentemente con l'attuale andamento delle tecnologie informatiche.

B.04 Accessi esterni non autorizzati

Ci si riferisce al caso in cui vi siano intrusioni via rete, avvenute senza furto di credenziali di autenticazione ma semplicemente mediante lo sfruttamento di difetti del software, per effettuare accessi non autorizzati ai dati.

Il Firewall centralizzato di alta affidabilità oltre ad impedire accessi dall'esterno ne traccia anche i tentativi.

C. EVENTI RICONDUCIBILI AL CONTESTO FISICO-AMBIENTALE-INFRASTRUTTURALE

C.01 Ingressi non autorizzati ad aree/locali ad accesso ristretto

Ci si riferisce alla concreta possibilità che soggetti non legittimati all'accesso possano materialmente accedere all'interno dei locali e degli Uffici in cui sono posizionati gli apparati e gli elaboratori informatici ospitanti i dati personali che formano oggetto di trattamento. In casi di questo tipo, il danno che può derivare non è solo quello, di per sé già molto grave, di accesso di soggetto non legittimato alle banche dati trattate dagli Uffici in quanto, si possono verificare anche ipotesi di modifica non autorizzata, di distruzione e conseguente perdita, di esportazione illegittima delle Banche Dati oggetto dell'evento dannoso considerato.

In relazione a tale possibilità la Camera di Commercio di Lucca ha provveduto alla protezione dei locali con apposite serrature le cui chiavi di accesso sono consegnate solo all'Amministratore di Sistema. E' inoltre stato installato allarme anti intrusione al piano terra dell'edificio.

C.02 Guasto a sistemi complementari (Impianto elettrico, climatizzazione)

Ci si riferisce a tutti quegli eventi che riguardando sistemi ed impianti esterni ma complementari agli strumenti informatici, vanno ad impattare sugli stessi inficiandone la funzionalità. Il tipico esempio di guasto a sistema complementare è quello che riguarda l'impianto elettrico ovvero l'impianto di climatizzazione.
Il rischio correlato a tale tipologia di evento è quello di danneggiamento dei dati e di indisponibilità temporanea, ovvero nei casi più gravi, permanente degli stessi.

- Blackout.

In relazione a tal guasti la Camera di Commercio di Lucca ha inserito un sistema di UPS (Gruppi di Continuità) per poter chiudere il lavoro correttamente durante l'eventuale Black-out.

C.03 Eventi distruttivi, naturali o artificiali accidentali o dovuti ad incuria

Include tutti gli eventi di effetto distruttivo sui supporti fisici contenenti i dati o sulle apparecchiature informatiche, indipendentemente dalla loro natura, qualora non siano già inclusi nelle casistiche precedenti.
Il rischio che si può determinare sui dati è quello di danneggiamento, indisponibilità temporanea o perdita parziale o totale degli stessi.

- Incendio parziale o diffuso;
- Scariche atmosferiche;
- Allagamenti;
- Condizioni ambientali estreme.
-

In relazione alla possibilità di allagamento, la Camera di Commercio di Lucca ha posto i computer non direttamente sul piano di calpestio, frapponendo un supporto ad hoc.

15.*2 Sicurezza Informatica*

L'accesso al sistema informatico dell'Ente viene garantito attraverso la verifica di apposite credenziali costituite da un codice identificativo (User ID) e da una password, attribuite in via esclusiva a ciascun dipendente individuato quale incaricato del trattamento dei dati e il Server di Dominio conserva tutte le informazioni sulle utenze e sui permessi di accesso alle risorse disponibili, previa verifica della validità delle login e delle password fornite dai Client.
Ogni utente risulta inserito in un Gruppo (relativo al settore di competenza) al fine di avere una serie di dati e cartelle per tutti gli utenti del servizio relativo.

La forma di protezione adottata per contrastare gli eventuali sbalzi di tensione elettrica, come già menzionato al paragrafo relativo, è rappresentata da singoli gruppi di continuità collegati, in locale ai Server e agli apparati di rete.

Come già anticipato nella sezione corrispondente, per la protezione da software dannosi, virus e malware, intrusioni dall'esterno, oltre all'installazione di antivirus in tutti i Client di Rete e sul Server (protezionelocale), è stata appositamente acquisito un Firewall che provvede anche alle protezioni Antivirus, AntiMalware, Anti Spam e Context Filtering per blocco accessi dall'interno della Rete LAN su siti Rischiosi per la navigazione, Pornografici, Pedopornografici, e comunque su siti non Etici.
Per la protezione da accessi non autorizzata da parte degli Amministratori di sistema è stato predisposto
un sistema SYSLOG, compatibile rispetto alle Normative sulla Privacy in merito alle Pubbliche Amministrazioni.

15.*3 Descrizione dei casi di disastro/indisponibilità.*

In questo paragrafo si trova una elencazione dei casi in cui sarà attivata la soluzione di DR per i servizi da erogare nel caso in cui si presenti l'indisponibilità del sistema informatico dell'Ente o un qualsivoglia problema legato ad esso. Nello specifico devono essere individuati i casi di disastro e/o di indisponibilità del sistema informatico dell'Ente in cui si provvederà all'attuazione della soluzione di DR.

Rischi considerati:

- Mancanza di erogazione del servizio dovuta all'impossibilità di accedere ai dati e alle banche
- dati;
- Distruzione delle infrastrutture IT ovvero del CED;
- Impossibilità di accedere al CED o ai locali destinati nei quali sono stati collocati server, apparati
- di rete e di backup;
- Mancanza di erogazione del servizio dovuta a un funzionamento non corretto degli applicativi
- gestionali utilizzati dai dipendenti dell'Ente.

16. ORGANIZZAZIONE E PERSONALE

Organizzazione, ruoli e responsabilità, strutture e personale coinvolto nelle attività.
In questa sezione vengono elencate tutte le persone e le figure con i relativi incarichi, dati anagrafici e contatti per le comunicazioni, che sono coinvolte nella gestione dell'emergenza e della soluzione di DR, comprensivo delle figure facenti parte del Comitato di Gestione Crisi.
Viene inoltre descritta la struttura di riferimento per la gestione della soluzione di DR con i rispettivi compiti e competenze.

Responsabile Continuità Operativa: provvede a contattare tutte le figure del Comitato di Gestione Crisi, secondo i modi e le modalità indicate nella tabella sottostante. Provvede a redigere le relazione da inviare all'Agenzia per l'Italia Digitale nei casi in cui sopraggiunga un disastro e sia necessario attivare la continuità operativa e il disaster recovery.

Comitato d i Gestione della Crisi:

Ufficio / Ruolo	Cognome/Nome	Tel. Ufficio	Cellulare

Responsabile Continuità Operativa	Claudio Mori	0583976612	3473663384
Segretario Generale	Roberto Camisi	0583976647	3293606491
Dirigente Settore Anagrafico e Regolazione del Mercato	Bruni Alessandra	0583976648	3389462182
Dirigente Area Amministrazione e Personale	Massimo Marsili	0583976438	3389326971
Provveditore	Luca Granucci	0583976614	

Amministratori di sistema: viene contattato dal RCO dell'Ente e si riunisce con il Comitato di Gestione Crisi per valutare l'entità dell'evento disastroso dichiarato. In seguito provvede al ripristino del sistema nella sede secondaria individuata, previa disponibilità delle risorse elaborative. Provvede inoltre alla configurazione dei server e dei personal computer per garantire livelli minimi di sicurezza e di inviolabilità del sistema anche in condizioni di emergenza.

Team operativo di Disaster Recovery

E' il gruppo di supporto competente per la riattivazione dei servizi informatici.

Ufficio / Ruolo	Cognome/Nome	Tel. Ufficio	Cellulare	Email
Provveditorato Funzioni Informatiche	Francesco Guidi	0583976695		

Ufficio Stampa

E' la funzione deputata alla gestione contatti con la stampa.

Ufficio / Ruolo	Cognome/Nome	Tel. Ufficio	Cellulare	Email
Ufficio Relazioni con l'Esterno	Francesca Sargenti	0583976686		
Ufficio Relazioni con l'Esterno	Delia Vecchi	058397661		

Fornitori

Denominazione : INFOCAMERE SCpA	
Provider ID	001
Descrizione	Società di Informatica delle Camere di Commercio italiane
Indirizzo	Corso Stati Uniti, 14 – 35127 PADOVA
Telefono	049-8089610

Fornitore di servizi; Infocamere, nel gestire la crisi, procede secondo quanto previsto dai suoi processi di gestione incident, problem management e gestione della crisi, basati su procedure interne Infocamere (procedura MG/7 e suoi allegati), certificate secondo standard ITIL e ISO27001 e documentate nei processi interni Infocamere. Il Piano di Continuità Operativa e il Piano di Disaster Recovery sono gestiti dalla stessa Infocamere.

Sintesi degli accordi contrattuali in essere:

Denominazione : Lucense S.c.p.A	
Provider ID	002
Descrizione	Lucense S.c.p.A
Indirizzo	Via della Chiesa XXXII, trav.I n.231, Sorbano del Giudice 55100 Lucca
Telefono	+39 0583 493616

In attesa di descrizione da parte di Lucense ScpA

Sintesi degli accordi contrattuali in essere:
I rapporti e gli aspetti contrattuali con la Società Lucense ScpA, relativamente alla fornitura del servizio in hosting del sito istituzionale , sono stati curati dall'Ufficio URE con i provvedimenti DD 92 del 18/03/2014 e 42 del 05/02/2015.
Il servizio è stato aggiudicato ricorrendo al portale MEPA.

Modalità di attivazione del personale.

Le figure e le persone citate nella sezione precedente devono essere contattate attraverso qualsiasi mezzo di comunicazione l'Ente e/o il Responsabile della Continuità Operativa possa utilizzare,
Il Comitato di Gestione Crisi provvederà ad informare il Responsabile dell'Area coinvolta ovvero tutti i responsabili in caso di evento dannoso diffuso, sul momento di rientro alla sede primaria e/o ad una diversa sede definitiva in caso d'indisponibilità di quella principale.

Il Comitato di Gestione Crisi stabilisce inoltre il momento di chiusura della crisi, comunicandolo alle funzioni coinvolte nelle operazioni di Recovery.

17. POLITICA DI SICUREZZA E DI SALVAGUARDIA DEI DATI

In questa sezione vengono descritte le procedure di backup e archiviazione dei dati poste in essere dall'Ente per evitare una qualsiasi perdita dei dati nel sito primario e di salvaguardia degli stessi attraverso la copia schedulata e custodita nella sede remota. Viene dato infatti forte rilievo non solo alle procedure, alla tempistica e alla schedulazione dei backup per la salvaguardia dei dati conservati e custoditi nel sito remoto, ma vengono descritte anche tutte le impostazioni e le configurazioni poste in essere per il backup dei dati presente nel sito primario.
Il backup è un punto fondamentale nelle procedure di disaster recovery e per garantire maggiori livelli di sicurezza è necessario che le copie di sicurezza dei dati siano collocate anche all'esterno dell'Ente, ovvero nella sede individuata quale sito di DR.
La Camera di Commercio di Lucca, come già meglio descritto in precedenza, per provvedere alla conservazione dei propri dati in luogo differente rispetto al sito di produzione si è dotato di un'infrastruttura in hosting ove si esegue automaticamente la replica/ridondanza dei server dati.
La conservazione delle copie di backup in locale, avviene tramite un'unità NAS (backup su file) e su unità su DAT (nastro magnetico). La copia a nastro viene poi successivamente conservata in un armadio a tenuta termica, risulta strettamente necessaria per evitare che, in caso di perdita di dati o di evento disastroso circoscritto ai soli locali ove vi stazionano i Server, le copie di sicurezza vadano perse. Il ripristino dei dati, detto restore, viene effettuato dall'amministratore del sistema informatico o da altri addetti analogamente abilitati all'accesso al sistema, che provvedono al ripristino dei file richiesti.
Attraverso i diversi software di backup operativo, Symantec Backup Exec 11d (relativo alle Copie su nastro), Symantec Backup Exec System Recovery su NAS, vengono eseguite le copie di sicurezza dei dati residenti nel Server Dati.

Le operazioni di backup sono eseguite automaticamente e ad intervalli prestabiliti come di seguito specificato:

Backup automatico completo: ore 23:00 di ogni giorno lavorativo della settimana.

18. FASI DELLA SOLUZIONE DI DISASTER RECOVERY

1. Valutazione della situazione di crisi/disastro/indisponibilità del sito primario;
2. Dichiarazione del disastro;
3. Notifica, informativa ed attivazione delle strutture e del personale coinvolto nelle attività connesse alla dichiarazione di disastro;
4. Attivazione del Piano di DR e delle procedure ad esso connesse;
5. Attivazione del sito di DR e ripristino del sistema informativo primario, colpiti dal disastro o dalla situazione di indisponibilità;
6. Gestione dei sistemi informativi presso il sito di DR in condizioni di emergenza, durante il periodo di disastro o indisponibilità;
7. Ripristino del sistema primario con la formale "Dichiarazione di fine emergenza" da parte del Comitato di Gestione Crisi.

Attivazione del Piano di DR e delle procedure ad esso connesse

La responsabilità di attivazione del Piano di Disaster Recovery è del Comitato di Gestione Crisi o di altra figura/persona delegata facente funzioni.

Attivazione del sito di DR e ripristino del sistema informativo primario, colpiti dal disastro o dalla situazione di indisponibilità

La tabella di seguito riportata descrive le attività da intraprendere per ripristinare il sistema informatico e per attivare il sito alternativo. Nella tabella sono inoltre riportati i responsabili delle rispettive attività; la parte descrittiva dovrà essere compilata ed allegata da parte dei vari responsabili che in caso di dichiarazione dell'emergenza dovranno dettagliare e specificare le decisioni prese.
Durante lo svolgimento delle attività è importante che il Responsabile della Continuità Operativa tenga traccia delle decisioni prese, delle spese sostenute e dell'effettivo consumo delle risorse (sia umane che materiali) utilizzate per ripristinare i servizi in modo tale da poter fornire, alla fine delle attività, un resoconto completo da allegare al Piano stesso e da inviare all'Agenzia per l'Italia Digitale.

STEP ATTIVITA' RESPONSABILE DESCRIZIONE

Step	Responsabile	Attività	Descrizione attività
1	Responsabile della Continuità Operativa	Rilevazione incidente	l'ufficio informatico, se l'incidente blocca le attività per più di 3 ore avvisa il RCO che decide se fare escalation e attivare il comitato di crisi
2	Responsabile della Continuità Operativa	Attivazione del Comitato di Crisi	se il responsabile del Comitato della Continuità Operativa ritiene significativa la gravità dell'incidente, dà inizio all'attivazione del Comitato di Crisi
3	Responsabile della Continuità Operativa	Convocazione del Comitato di Crisi	Convocazione del Comitato di Crisi

4	Responsabile Comunicazione	Informare il Consiglio Camerale e la Giunta della crisi in atto	Inviare nota al Consiglio Camerale ed alla Giunta
5	Responsabile Continuità Operativa	Valutazione l'accessibilità ai sistemi e alle apparecchiature necessarie a garantire i servizi IT	Eseguire una approfondita valutazione dei sistemi del sito primario e produrre un rapporto nel quale indicare: principali rischi individuati ed eventuali politiche preliminari per la loro minimizzazione; le aree che dovranno essere monitorate per la sicurezza ed integrità dell'IT. Richiedere eventuali valutazioni aggiuntive specifiche ad esperti esterni. Attivare la Procedura di Comunicazione.
6	-Responsabile Continuità Operativa - Referente Ufficio Servizi Informatici	Definizione la soluzione da adottare	Decidere se attivare il sito secondario oppure riattivare il sito primario oppure intraprendere altre soluzioni. Le azioni previste dovranno includere: • Predisposizione di stazioni di lavoro (Ufficio Servizi Informatici - Referente Informatico Infocamere) • Eventuali spese di funzionamento urgenti (RCO - Provveditore) • Supporto logistico (Ufficio Tecnico)
7	- Responsabile Continuità Operativa - Referente Ufficio Servizi Informatici	Comunicazione ai fornitori sulla situazione di crisi e la necessità di dare supporto all'attivazione del sito secondario	Contattare i principali fornitori per avvertirli della crisi aziendale e richiedere loro la disponibilità a fornire una corsia preferenziale ad eventuali richieste dovessero rendersi necessarie. Per l'elenco fornitori si rimanda al cap. 8 "Fornitori"
8	Responsabile Continuità Operativa	Contattare il fornitore InfoCamere SCPA	Contattare il fornitore InfoCamere SCPA per attivare il sito secondario e richiedere, in caso di danneggiamento, la sostituzione nell'arco di 24 ore degli degli apparati attivi e ruouter
9	Responsabile Continuità Operativa	Attivazione sito secondario DR	Richiedere a InfoCamere SCPA l'attivazione sito secondario di DR
10	Responsabile Continuità Operativa	Ripristino attività tramite sito secondario DR	Avvio ripristino attività tramite la messa in funzione del sito secondario DR
11	Responsabile Continuità Operativa	Avvio attività di ripristino sito primario	
12	Responsabile Continuità Operativa	Dichiarazione di fine emergenza	Verifica del completo ripristino delle attività del sito primario

19. PROCEDURE DI TEST

L'Ente deve prevedere e provvedere all'esecuzione di test periodici ed operativi in modo che sia garantito l'aggiornamento e il controllo dei piani; le modifiche del piano di Disaster Recovery saranno effettuate ogni qualvolta venga acquistata una nuova apparecchiatura o elaboratore elettronico per adeguamento del sistema informatico che vadano a impattare sull'attuazione della soluzione tecnologica. Oltre all'adeguamento tecnologico del sistema informatico si dovrà provvedere all'aggiornamento del Piano di DR anche nel caso in cui si modifichi la metodologia utilizzata per il disaster recovery; questo dovrà essere controllato nel corso dei test periodici che dovranno essere relazionati e inseriti nel Piano.
Possono comunque verificarsi condizioni che richiedono specifiche procedure di manutenzione straordinaria per cui si dovrà provvedere ad un adeguamento del Piano:
· modifiche delle figure facenti parte del Comitato di Gestione Crisi;
· modifiche dei Responsabili delle Aree/Servizi;
· modifiche legate ai gestionali utilizzati dall'Ente e/o al fornitore;
· modifica dell'amministratore di sistema;
· modifica del fornitore dei servizi

L'Ente deve provvedere, periodicamente, ad effettuare i test di verifica e corretto funzionamento della soluzione di disaster recovery. I test consistono nelle seguenti simulazioni sul sito di DR:
· Il Responsabile della CO, esegue Comunicazione del Test di DR ai Responsabili di Area.
· Il Responsabile della CO attiva il Piano di DR nelle modalità operative simulate.
· L'Amministratore di Sistema controlla l'effettivo aggiornamento dei dati estraendone una serie significativa a campione.
Queste verifiche devono essere eseguite in considerazione delle tempistiche di aggiornamento del sito di DR concordate con il Provider.
Alla conclusione delle procedure di test deve essere redatta una relazione, a cura del Responsabile della Continuità Operativa e conservata agli atti, la quale deve essere fornita in copia alle figure che compongono il Comitato di Gestione Crisi.
La suddetta relazione deve descrivere i procedimenti effettuati per il test del disaster recovery e deve evidenziare gli eventuali discostamenti dal corretto andamento delle procedure.

SCENARIO A: PERDITA SITO PRIMARIO
La simulazione della perdita ovvero dell'impossibilità all'utilizzo del Server, consiste in:
· interruzione della sincronizzazione delle copie di sicurezza e dei riallineamento dei dati effettuate presso la sede remota;
· procedure di collegamento del sistema remoto (sul sito di DR);
· procedura di avvio degli applicativi;
· procedura di avvio del singolo servizio o dei servizi;
· procedura di verifica degli applicativi testati;
· procedure di ripristino della soluzione di disaster recovery.

SCENARIO B: DATA RECOVERY

La simulazione della perdita dei dati, consiste in:
· interruzione della sincronizzazione delle copie di sicurezza e dei riallineamento dei dati effettuate presso la sede di DR;
· procedure di collegamento del sistema remoto (sul sito di DR);

· procedure di recupero o di acquisizione di nuove apparecchiature elettroniche se necessario;
· procedure di ripristino della soluzione di disaster recovery.