

Piano di Continuità Operativa

08/01/2018

“Continuità operativa” C.A.D. ex Art. 50 bis

Versione Documento	0.1
Data emissione	08/01/2018
Redatto da :	RCO – Franca Tiloca in collaborazione con Infocamere
Verificato da :	RCO – F.Tiloca, Provveditore – L.Nughes, Informatico – G. Rosa, Segretario Generale -P. Esposito
Approvato da :	Segretario Generale – P. Esposito
Autorizzato da :	Segretario Generale – P. Esposito

PCO CCIAA SASSARI

Plan Last Updated: 08 Jan 2018

PCO Sassari

Exported By: Corrado Claut

Exported On: 08 Jan 2018

Piano di Continuità Operativa per le CCIAA

Business Continuity

Table Of Contents

Report/Document Name	Page
01 Storia delle Modifiche Apportate	1

02 Generalità	2

03 Posizionamento del presente documento	7

04 Definizioni del Piano di Continuità Operativa	11

05 Siti nel Piano	15

06 Servizi forniti da Infocamere	17

07 Servizi forniti da altri Fornitori	24

08 PCO - 1. Fase Reazione Emergenza **25**

08 PCO - 2. Fase Gestione Emergenza **31**

08 PCO - 3. Fase Chiusura Emergenza **33**

09 Team Ruoli Risorse **34**

10 Fornitori **37**

11 Riferimenti normativi **39**

12 Elenco Personale nel Piano **41**

01 Storia delle Modifiche Apportate

Exported On: 8 Jan 2018

Nome del Piano: PCO Sassari

GESTIONE DEL PIANO

STORIA DELLE MODIFICHE APPORTATE

Copia del piano di continuità sarà approvata, con cadenza almeno biennale, dal Segretario Generale dell'Ente d'impulso RCO (Reasponsabile della continuità Operativa).

Per rendere più rapido il ciclo di revisione del documento a fronte di variazioni secondarie (quali ad es. l'aggiornamento dei riferimenti) e non di processo, l'approvazione sarà limitata alla Responsabile della Continuità Operativa.

Nome del Piano: PCO Sassari

Introduzione: 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'ex articolo 50-bis del CAD (abrogato con DLGS 27/08/2016 n.179) delineava 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 stato acquisito il parere di Agenzia per l'Italia.

Obiettivo del Piano di Continuità Operativa ICT

Il presente Piano di Continuità Operativa (in seguito PCO) 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 presente PCO prevede 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.

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 Sassari.

La prima versione del documento è stata redatta dal RCO e approvata dal Segretario Generale dell'Ente, 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.

Assunzioni: Validità

Destinatari del Piano di Continuità Operativa della Camera Commercio di Sassari, 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 Sassari il ruolo è svolto dalla **Dott.ssa Franca Tiloca**, nominata con determinazione dirigenziale num.

517 del 31/12/2014.

- 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.

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. 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).

Gestione delle reperibilità

Sono sempre reperibili sia il dirigente, dott. Pietro Esposito, Segretario Generale dell'ente, che la funzionaria camerale dott.ssa Franca Tiloca, Responsabile della Continuità Operativa e il dott. Leonardo Nughes, Provveditore.

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

-nel fine settimana (ven sab dom) è reperibile telefonicamente il Segretario Generale. Sono inoltre reperibili il Responsabile della continuità operativa ed il Provveditore. Il Segretario Generale, il Provveditore ed il RCO formano il Team di coordinamento crisi.

Formazione

Le procedure previste per la Continuità Operativa saranno divulgate nelle seguenti modalità: -nella versione originale con incontro annuale tra il Segretario Generale, il Responsabile della continuità operativa ed il Provveditore 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.

Schedulazioni richieste: Testing

Il test periodico prevede:

-riunione annuale tra Segretario Generale, Responsabile della continuità operativa e Provveditore. -contatto dei fornitori per verifica disponibilità hardware compatibile con le esigenze previste nel documento di ripristino file server.

Gestione ed aggiornamento del Piano di Continuità Operativa

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 Segretario Generale nella prevista riunione annuale o in apposita riunione convocata qualora se ne presenti la necessità.

03 Posizionamento del presente documento

Exported On: 8 Jan 2018

Nome del Piano: PCO Sassari

ESTRATTO STUDIO DI FATTIBILITÀ TECNICA

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 Sassari ad AgID in data 08/07/2015 prot. n. 12867.

Sintesi del parere di AGID

Nel parere n. 1072/2015 emesso da parte di AgID il 24/09/2015, ed inviato alla Camera Commercio di Sassari il 05/10/2015 con prot n. 17389 si esprime quanto segue:

CONSIDERATO

Considerazioni generali di natura strategica

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 Sassari per l'attuazione del CAD e la digitalizzazione dei procedimenti amministrativi.

Analisi tecnica SFT e soluzione di DR proposta/adottata

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 20; i servizi posti in ambito sono 17.

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.

Osservazioni sulle soluzioni tecniche proposte

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

L'Amministrazione, per quanto concerne le Soluzioni Tecnologiche Tier 4/IC-A e C, dà indicazioni in merito al sito secondario, indicando la distanza di quest'ultimo dal sito primario; mentre, per quanto concerne la Soluzione Tecnologica Tier 2/CCIAA-A, dichiara che alla data di predisposizione dello Studio di Fattibilità Tecnica, il sito di DR non risulta previsto in quanto non sono disponibili le risorse necessarie.

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:

-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/Rac...>, 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

ESTRATTO STUDIO DI FATTIBILITÀ TECNICA

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.

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.

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 3 soluzioni: la soluzione tecnologica Tier 4/IC-A, la Tier 4/IC-C e la Tier 2/CCIAA-A.

Tali soluzioni sono coerenti e migliorative, rispetto ai Tier suggeriti dal tool di autovalutazione. Si osserva che, per quanto concerne la Soluzione tecnologica CCIAA-A, l'Amministrazione riferisce che la stessa è caratterizzata dal Tier 2 indicando, invece, come modalità di trasferimento dati fra siti, la connessione di rete. Si ricorda all'Amministrazione che la principale differenza fra il Tier 2 ed il Tier 3 risiede proprio nel fatto che, per quest'ultimo, il trasferimento dei dati fra il sito primario e quello di DR avviene attraverso un collegamento di rete fra i due siti.

Valutazione dell'omogeneità delle soluzioni prescelte rispetto a quelle di altre Amministrazioni Le soluzioni previste dalla Camera di Commercio di Sassari sono omogenee a quelle di altre amministrazioni simili.

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 dalla Camera di Commercio di Sassari 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 Tier 4/IC-A e Tier 4/IC-C, 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) 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; 5) venga verificato, nell'implementazione delle soluzioni tecniche di DR descritte, che le stesse siano effettivamente in grado di rispondere alle esigenze di CO con particolare riferimento ai tempi massimi di ripristino (RTO) e di perdita massima di dati accettata (RPO);
- 6) 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).

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:

- I Servizi
 - **Gestione documentale,**
 - **Altri Registri, Albi e Ruoli,**
 - **Vigilanza e controllo prodotti, metrologia legale e certificati origine merci** elencati nella soluzione tecnologica Tier 4/IC-C dello Studio sono stati posti in regime di CO/DR
- I **Servizi per l'Ambiente**, citati all'interno della soluzione tecnologica Tier 4 / IC-C dello Studio, sono attualmente in fase di migrazione verso l'ambiente di CO/DR
- La classe di Servizi **Marchi e Brevetti** viene eliminata, in quanto da più di un anno i corrispondenti servizi sono passati direttamente in capo, sia come erogazione che come gestione, al Ministero dello Sviluppo Economico (piattaforma UIMB)

04 Definizioni del Piano di Continuità Operativa

Exported On: 8 Jan 2018

Tipo: 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.
PCO [Piano di Continuità Operativa]	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"

PDR [Piano di Disaster Recovery]	<p>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.</p> <p>Si evidenzia che il PDR è la sezione del PCO che descrive le attività di ripristino del sistema informativo.</p>
----------------------------------	--

Tipo: Definizioni

TERMINE / ACRONIMO	DEFINIZIONE
RCO [Responsabile Continuità Operativa]	<p>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 è membro del Comitato di crisi.</p> <p>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:</p> <ul style="list-style-type: none">- 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. <p>Qualora la situazione di emergenza ICT si prolunghi oltre quanto previsto, il responsabile della Continuità Operativa deve valutare le azioni gestionali/comunicative, amministrative più opportune.</p>
RPO [Recovery Point Object]	Rappresenta il massimo tempo che intercorre tra la produzione di un dato e la sua messa in sicurezza .
RTO [Recovery Time Object]	Tempo atteso per il ripristino dei servizi critici sul sito di DR.
TERMINE / ACRONIMO	DEFINIZIONE

Tipo: Definizioni

SCENARIO D1	<p>Le condizioni cui far fronte sono:</p> <ul style="list-style-type: none">● Strumentazione tecnologica completamente inutilizzabile e/o isolata dal punto di vista della connettività di rete Sede della● Camera di Commercio inagibile (disastro strutturale / ambientale) <p>A titolo di esempio si riporta una serie di eventi associati allo tipologia di scenario D1:</p> <ul style="list-style-type: none">● Alluvione estesa● Incendio esteso● Terremoto distruttivo
SCENARIO D2	<p>Le condizioni cui far fronte sono:</p> <ul style="list-style-type: none">● Strumentazione tecnologica completamente inutilizzabile e/o isolata dal punto di vista della connettività di rete Sede della● Camera di Commercio agibile <p>A titolo di esempio si riporta una serie di eventi associati allo tipologia di scenario D2:</p> <ul style="list-style-type: none">● Alluvione parziale● Crollo parziale della struttura● Mancanza di elettricità● Incendio● Perdita di connettività di rete
TERMINE / ACRONIMO	DEFINIZIONE

Tipo: Definizioni

SCENARIO D3	<p>Le condizioni cui far fronte sono:</p> <ul style="list-style-type: none">● Infrastruttura tecnologica parzialmente inutilizzabile● Sede della Camera di Commercio agibile <p>A titolo di esempio si riporta una serie di eventi associati allo tipologia di scenario D3:</p> <ul style="list-style-type: none">● 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, sgombrò locali, movimentazione arredi ecc.)

05 Siti nel Piano

Exported On: 8 Jan 2018

NOME DEL SITO	CdC Sassari – Sede centrale
----------------------	-----------------------------

INDIRIZZO	Via Roma 74
------------------	-------------

CITTÀ	Sassari
--------------	---------

PROVINCIA	SS
------------------	----

CODICE POSTALE	
-----------------------	--

TELEFONO	079/2080361
-----------------	-------------

FUNZIONE PRINCIPALE	Sede Primaria
----------------------------	---------------

INFORMAZIONI ADDIZIONALI	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.
---------------------------------	--

NOME DEL SITO	CdC Sassari – Sede secondaria di Olbia
----------------------	--

INDIRIZZO	Via Capoverde, angolo Via Seychelles, Zona Industriale settore 4 c/o Delta Center
------------------	--

CITTÀ	Olbia
--------------	-------

PROVINCIA	SS
------------------	----

CODICE POSTALE	
-----------------------	--

TELEFONO	0789 69580
-----------------	------------

FUNZIONE PRINCIPALE	Sede Secondaria
----------------------------	-----------------

NOME DEL SITO	CdC Sassari – Sede secondaria di Predda Niedda “Promocamera”(già sede dell’azienda speciale)
INFORMAZIONI ADDIZIONALI	<p>Si riportano le caratteristiche dettagliate di questa sede secondaria :</p> <p>Infrastrutture di continuità e protezione fisica L’armadio tecnologico e i PC sono dotati 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 Sassari, sono a disposizione del Responsabile della sede di Olbia. Ambiente logistico (interno) per la continuità Presso la sede di <i>Olbia</i> è disponibile una stanza con 5 scrivanie e 5 postazioni di lavoro. Lo switch in dotazione presso questa sede ha 8 ingressi liberi, è quindi possibile espandere il numero di postazioni.</p>

INDIRIZZO	Regione Predda Niedda, 18 - “Promocamera”	CITTÀ	Sassari
PROVINCIA	SS	CODICE POSTALE	
TELEFONO	079 2638800	FUNZIONE PRINCIPALE	Sede Secondaria
INFORMAZIONI ADDIZIONALI	<p>Qualora l’indisponibilità della sede primaria si protragga per più di 3 settimane, il Segretario Generale potrà disporre l’attivazione di num. 5 postazioni di lavoro per lo svolgimento delle attività presso la sede di <i>Sassari Predda Niedda, 18 “Promocamera”</i> .</p>		

06 Servizi forniti da Infocamere

Exported On: 8 Jan 2018

CLASSE DI SERVIZIO: Altri Registri albi e ruoli [Italiancom]

Descrizione: 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

SERVIZIO	TIPOLOGIA DI UTENZA	INDICE COMPLESSIVO CRITICITA	CLASSE CRITICITA	SOLUZIONE TECNOLOGICA	RPO	RTO
Imprese operanti con l'estero [ItalianCom]	Eterogenea (Cittadini, Imprese, P.A.)	4	Media	Tier 2	24 Hours	72 Hours

CLASSE DI SERVIZIO: Archivio PARD e Albi Camerali

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

SERVIZIO	TIPOLOGIA DI UTENZA	INDICE COMPLESSIVO CRITICITA	CLASSE CRITICITA	SOLUZIONE TECNOLOGICA	RPO	RTO
Albi Camerali - Alca	Eterogenea (Cittadini, Imprese, P.A.)	5	Media	Tier 4	4 Hours	72 Hours
Artigiani	Eterogenea (Cittadini, Imprese, P.A.)	5	Media	Tier 4	4 Hours	72 Hours

CLASSE DI SERVIZIO:**Descrizione:****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 c

SERVIZIO	TIPOLOGIA DI UTENZA	INDICE COMPLESSIVO CRITICITA	CLASSE CRITICITA	SOLUZIONE TECNOLOGICA	RPO	RTO
Carte Tachigrafiche	Eterogenea (Cittadini, Imprese, P.A.)	5	Media	Tier 3	24 Hours	72 Hours

CLASSE DI SERVIZIO: Contabilità, Pianificazione, Controllo di Gestione ed Amministrazione Aperta

Descrizione: Tenuta della contabilità, pianificazione e controllo di gestione, gestione del ciclo di spesa e di investimento, amministrazione e gestione del personale CCIAA

SERVIZIO	TIPOLOGIA DI UTENZA	INDICE COMPLESSIVO CRITICITA	CLASSE CRITICITA	SOLUZIONE TECNOLOGICA	RPO	RTO
Pubblicamera	Eterogenea (Cittadini, Imprese, P.A.)	5	Media	Tier 4	24 Hours	72 Hours
Sistema Gestione Amministrazione del Personale - Sipert	Eterogenea (Cittadini, Imprese, P.A.)	5	Media	Tier 4	24 Hours	72 Hours
Sistemi per la Gestione Amministrativo - Contabile	Eterogenea (Cittadini, Imprese, P.A.)	5	Media	Tier 4	24 Hours	72 Hours

CLASSE DI SERVIZIO:**Descrizione:**

Diritto Annuale

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

SERVIZIO	TIPOLOGIA DI UTENZA	INDICE COMPLESSIVO CRITICITA	CLASSE CRITICITA	SOLUZIONE TECNOLOGICA	RPO	RTO
Diritto Annuale e sanzioni	Eterogenea (Cittadini, Imprese, P.A.)	5	Media	Tier 3	24 Hours	72 Hours

CLASSE DI SERVIZIO: Registro Imprese

Descrizione: 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

SERVIZIO	TIPOLOGIA DI UTENZA	INDICE COMPLESSIVO CRITICITA	CLASSE CRITICITA	SOLUZIONE TECNOLOGICA	RPO	RTO
Registro Imprese - Elaborazioni batch	Eterogenea (Cittadini, Imprese, P.A.)	5	Media	Tier 4	4 Hours	72 Hours
Registro Imprese - Interrogazioni	Eterogenea (Cittadini, Imprese, P.A.)	5	Media	Tier 4	4 Hours	72 Hours
Registro Imprese - Istruttoria	Eterogenea (Cittadini, Imprese, P.A.)	5	Media	Tier 4	4 Hours	72 Hours
Registro Imprese - Pratiche	Eterogenea (Cittadini, Imprese, P.A.)	5	Media	Tier 4	4 Hours	72 Hours

CLASSE DI SERVIZIO:**Descrizione:**

Registro Imprese Servizi per l'efficienza	Eterogenea (Cittadini, Imprese, P.A.)	5	Media	Tier 4	4 Hours	72 Hours
Registro Imprese - Servizi Statistici	Eterogenea (Cittadini, Imprese, P.A.)	5	Media	Tier 4	4 Hours	72 Hours
Registro Imprese - Telemaco	Eterogenea (Cittadini, Imprese, P.A.)	5	Media	Tier 4	4 Hours	72 Hours

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

SERVIZIO	TIPOLOGIA DI UTENZA	INDICE COMPLESSIVO CRITICITA	CLASSE CRITICITA	SOLUZIONE TECNOLOGICA	RPO	RTO
Registro Informatico dei Protesti	Eterogenea (Cittadini, Imprese, P.A.)	5	Media	Tier 3	24 Hours	72 Hours

CLASSE DI SERVIZIO: Rete Telematica e Servizi di Connettività [Internet, Posta Elettronica]

SERVIZIO	TIPOLOGIA DI UTENZA	INDICE COMPLESSIVO CRITICITA	CLASSE CRITICITA	SOLUZIONE TECNOLOGICA	RPO	RTO
Sanzioni Amministrative – Accesa	Eterogenea (Cittadini, Imprese, P.A.)	5	Media	Tier 3	Hours	Hours

CLASSE DI SERVIZIO:**Descrizione:**

Descrizione: 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	TIPOLOGIA DI UTENZA	INDICE COMPLESSIVO CRITICITA	CLASSE CRITICITA	SOLUZIONE TECNOLOGICA	RPO	RTO
Servizi Tecnologici INTERNET (Internet e Posta)	Eterogenea (Cittadini, Imprese, P.A.)	6	Alta	Tier 4	24 Hours	72 Hours

CLASSE DI SERVIZIO: Sanzioni Amministrative

Descrizione: Sanzioni Amministrative erogate dalle CCIAA

Servizi di Conciliazione ed Arbitrato

Gestione delle Conciliazioni e arbitrato (CONCILIA)

SERVIZIO	TIPOLOGIA DI UTENZA	INDICE COMPLESSIVO CRITICITA	CLASSE CRITICITA	SOLUZIONE TECNOLOGICA	RPO	RTO
Mediazione Camerale	Eterogenea (Cittadini, Imprese, P.A.)	5	Media	Tier 3	24 Hours	72 Hours

CLASSE DI SERVIZIO: Servizi di Gestione Documentale

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

CLASSE DI SERVIZIO:**Descrizione:**

SERVIZIO	TIPOLOGIA DI UTENZA	INDICE COMPLESSIVO CRITICITA	CLASSE CRITICITA	SOLUZIONE TECNOLOGICA	RPO	RTO
Servizi di gestione documentale (Sistema di WorkFlow, Sistema di Gestione Documentale - LegalCycle - GeDoc)	Eterogenea (Cittadini, Imprese, P.A.)	5	Media	Tier 4	4 Hours	72 Hours

CLASSE DI SERVIZIO: Servizi per l'Ambiente**Descrizione:** Servizi legati alla salvaguardia ambientale

SERVIZIO	TIPOLOGIA DI UTENZA	INDICE COMPLESSIVO CRITICITA	CLASSE CRITICITA	SOLUZIONE TECNOLOGICA	RPO	RTO
----------	---------------------	------------------------------	------------------	-----------------------	-----	-----

Servizi per l'Ambiente

Servizi legati alla salvaguardia ambientale

SERVIZIO	TIPOLOGIA DI UTENZA	INDICE COMPLESSIVO CRITICITA	CLASSE CRITICITA	SOLUZIONE TECNOLOGICA	RPO	RTO
MUD - Modello Unico di dichiarazione Ambientale	Eterogenea (Cittadini, Imprese, P.A.)	5	Media	Tier 3	24 Hours	72 Hours
Pile	Eterogenea (Cittadini, Imprese, P.A.)	5	Media	Tier 3	24 Hours	72 Hours

CLASSE DI SERVIZIO:**Descrizione:**

RAEE - Registro Nazionale Trattamento Rifiuti di apparecchiature elettriche ed elettroniche	Eterogenea (Cittadini, Imprese, P.A.)	5	Media	Tier 3	24 Hours	72 Hours
SISTR1 - Sistema Tracciabilità Rifiuti	Eterogenea (Cittadini, Imprese, P.A.)	5	Media	Tier 3	24 Hours	72 Hours

CLASSE DI SERVIZIO: Vigilanza e Controllo Prodotti, Metrologia Legale e Certificati Origine Merci**Descrizione:** Vigilanza e controllo sui prodotti e per la metrologia legale e rilascio dei certificati di origine delle merci

SERVIZIO	TIPOLOGIA DI UTENZA	INDICE COMPLESSIVO CRITICITA	CLASSE CRITICITA	SOLUZIONE TECNOLOGICA	RPO	RTO
Albo Imbottiglieratori	Eterogenea (Cittadini, Imprese, P.A.)	4	Media	Tier 2	24 Hours	72 Hours
Certificazione prodotto tipici - ICDeis	Eterogenea (Cittadini, Imprese, P.A.)	4	Media	Tier 2	24 Hours	72 Hours

Vigilanza e Controllo Prodotti, Metrologia Legale e Certificati Origine Merci

Descrizione: Vigilanza e controllo sui prodotti e per la metrologia legale e rilascio dei certificati di origine delle merci

SERVIZIO	TIPOLOGIA DI UTENZA	INDICE COMPLESSIVO CRITICITA	CLASSE CRITICITA	SOLUZIONE TECNOLOGICA	RPO	RTO
Gestione Servizio Metrico - Eureka	Eterogenea (Cittadini, Imprese, P.A.)	4	Media	Tier 2	24 Hours	72 Hours

CLASSE DI SERVIZIO:

07 Servizi forniti da altri Forinatori

Exported On: 8 Jan 2018

CLASSE DI SERVIZIO: Sito web istituzionale

.....

Descrizione: Sito istituzionale <https://www.ss.camcom.it>

SERVIZIO	FORNITORE	TIPOLOGIA DI UTENZA	INDICE COMPLESSIVO CRITICITA	CLASSE CRITICITA	SOLUZIONE TECNOLOGICA	RPO	RTO
Sito web istituzionale	Uno srl	Eterogenea (cittadini, imprese, P.A.)	3	Media	TIER 3	24 Hours	24 Hours

Nome sottoattività:

08 PCO - 1. Fase Reazione Emergenza

Exported On: 8 Jan 2018

Tasks and Subtasks selected directly to Plans

Nome del Piano: PCO Sassari

Nome Attività: Fase di reazione all'emergenza

Descrizione: La struttura organizzativa

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

Descrizione dello specifico piano:

- Rilevazione incidente: l'ufficio informatico, coordinato dal Provveditore, se l'incidente blocca le attività per più di 3 ore avvisa il RCO che decide se fare escalation e attivare il team di coordinamento crisi;
- Valutazione: il RCO valuta se procedere ad escalation comunicando il problema al Segretario Generale;
- Attivazione del team di coordinamento crisi: se il responsabile della Continuità Operativa ritiene significativa la gravità dell'incidente, attiva il team di coordinamento crisi;

01 - Analizzare la criticità e dichiarare lo stato di crisi

Referente: Responsabile Continuità Operativa / Segretario Generale / Presidente (Rappresentante Legale)

Descrizione: 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:

- 1 D1 - Disastro Grave
- 2 D2 - Disastro Tecnologico
- 3 D3 - Gravi Danni Parziali

In caso di disservizio nel paragrafo "Elenco Servizi_Generalità" 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 paragrafo Fornitori.

ULTERIORI INFORMAZIONI

per il servizio "SITO WEB ISTITUZIONALE", fornito dalla Società "Uno srl", si richiede al fornitore di intervenire secondo gli accordi contrattuali in essere.

Competenza:

- Responsabile Continuità Operativa
- Segretario Generale
- Presidente (Rappresentante Legale)

Nome sottoattività: 02 - Attivare il centro controllo

Referente: Segretario Generale

Descrizione: 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.

Nome sottoattività:

ULTERIORI INFORMAZIONI

Nome sottoattività: 02 - Attivare il centro controllo

Referente: Segretario Generale

Descrizione: 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.

ULTERIORI INFORMAZIONI

Competenza:

- Segretario Generale
-

Nome sottoattività: 03 - Convocare il Comitato di Crisi

Referente: Responsabile Continuità Operativa

Descrizione: Convocare il Comitato di Crisi presso il Centro di Controllo

ULTERIORI INFORMAZIONI

Competenza:

- Responsabile Continuità Operativa
-

Nome sottoattività: 04 - Informare il Consiglio Camerale e la Giunta della crisi in atto

Referente: Segretario Generale

Descrizione: Inviare nota al Consiglio Camerale ed alla Giunta

ULTERIORI INFORMAZIONI

Competenza:

- Presidente (Rappresentante Legale)
-

Nome sottoattività: 05 - Mettere in atto le misure di sicurezza per garantire l'accesso ai siti primario e/o secondario

Referente: Segretario Generale

Descrizione: 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.

ULTERIORI INFORMAZIONI

Competenza:

- Provveditore in coordinamento con il Responsabile Sicurezza

06 - Ordinare l'evacuazione del sito primario e verificare l'accessibilità del sito secondario

Referente: Segretario Generale

Descrizione: 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.

ULTERIORI INFORMAZIONI

Competenza:

- Provveditore in coordinamento con il Responsabile Sicurezza

Nome sottoattività: 07 - Valutare l'accessibilità ai sistemi e alle apparecchiature necessarie a garantire i servizi IT con eventuale ausilio di personale esterno

Referente: Segretario Generale

Descrizione: 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.

ULTERIORI INFORMAZIONI

Competenza:

- Provveditore

Nome sottoattività: 08 - Raccogliere tutti gli elementi necessari ad individuare il piano di soluzione della crisi

Referente: Segretario Generale

Nome sottoattività:

Descrizione: 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.

ULTERIORI INFORMAZIONI

Competenza:

- Provveditore in coordinamento con il Referente Informatico e il Responsabile Continuità Operativa

Nome sottoattività: 09 - Valutare gli impatti sulle risorse infrastrutturali, economiche, umane e legali

Referente: Segretario Generale

Descrizione: Verificare la effettiva disponibilità delle persone necessarie per la attivazione del Sito Secondario (vedi Call List).

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.

ULTERIORI INFORMAZIONI

Competenza:

- Segretario Generale
- Responsabile Continuità Operativa
- Provveditore

Nome sottoattività: 10 - Definire la soluzione da adottare

Referente: Segretario Generale / Responsabile Continuità Operativa

Descrizione: Decidere se attivare il sito secondario (Contingency 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/Infocamera)
- Eventuali spese di funzionamento urgenti (Responsabile della Continuità Operativa - Provveditore)

- Supporto logistico (Ufficio Tecnico)

ULTERIORI INFORMAZIONI

Competenza:

- Referente Informatico
- Referente Informatico IC
- Provveditore
- Responsabile Sicurezza
- Segretario Generale

11 - Attivare le comunicazioni interne ed esterne relative

Referente: Segretario Generale

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

ULTERIORI INFORMAZIONI

Competenza:

- Segretario Generale
-

Nome sottoattività:

08 PCO - 2. Fase Gestione Emergenza

Exported On: 8 Jan 2018

Nome del Piano: PCO Sassari

Nome Attività: Gestione dell'emergenza

Descrizione: Questa fase permette di attivare il sito alternativo.

Nome sottoattività: 1 - Convocare le persone tecniche necessarie con eventuale trasferimento nel sito secondario

Referente: Segretario Generale

Descrizione: 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.

ULTERIORI INFORMAZIONI

Competenza:

- Responsabile Continuità Operativa
 - Provveditore
-

Nome sottoattività: 2 - Comunicare ai fornitori la situazione di crisi e la necessità di dare supporto alla attivazione del sito

Referente: Segretario Generale

Descrizione: 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 paragrafo "Fornitori"

ULTERIORI INFORMAZIONI

Competenza:

- Responsabile Continuità Operativa

3 - Attivare il piano di Disaster Recovery Tecnologico, solo in caso di attivazione sito secondario

Referente: Segretario Generale

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

Eeguire le attività di ripristino in Piano.

Controllare lo stato avanzamento delle attività del Contingency Plan.

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

ULTERIORI INFORMAZIONI

Competenza:

- Responsabile Continuità Operativa

Nome sottoattività: 4 - Eseguire il piano di DR (solo in caso di attivazione sito secondario) ed informare il Comitato di Crisi

Referente: Responsabile Continuità Operativa

Descrizione: 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.

Verifica il rispetto del RTO.

ULTERIORI INFORMAZIONI

Competenza:

- Referente Informatico
- Referente Informatico IC
- Provveditore

08 PCO - 3. Fase Chiusura Emergenza

Exported On: 8 Jan 2018

Nome sottoattività:

Nome del Piano: PCO Sassari

Nome Attività: Chiusura dell'emergenza

Descrizione: 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.

Nome sottoattività: 1 - Comunicazione interna di chiusura della crisi con indicazione dei limiti imposti dalla situazione di crisi

Referente: Segretario Generale

Descrizione: 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)

ULTERIORI INFORMAZIONI

Competenza:

- Responsabile Continuità Operativa
-

Nome sottoattività: 2 - Comunicazione esterna chiusura crisi

Referente: Segretario Generale

Descrizione: 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.

ULTERIORI INFORMAZIONI

Competenza:

- Segretario Generale
-

09 Team Ruoli Risorse

Exported On: 8 Jan 2018

Team: Ruoli di responsabilità e competenza

Descrizione:: No Descrizione: defined

COGNOME	Crobu	NOME	Luca		
RUOLO:	Responsabile Sicurezza				
TELEFONO LAVORO		CELLULARE		MAIL LAVORO	
UFFICIO COMPETENTE					
COGNOME	Esposito	NOME	Pietro		
RUOLO:	Segretario Generale				
TELEFONO LAVORO		CELLULARE		MAIL LAVORO	pietro.esposito@ss.camcom.it
UFFICIO COMPETENTE					
COGNOME	Nughes	NOME	Leonardo		
RUOLO:	Provveditore				
TELEFONO		CELLULARE		MAIL LAVORO	leonardo.nughes@ss.ca

LAVORO				mcom.it
UFFICIO COMPETENTE				

Team: Ruoli di responsabilità e competenza

Descrizione:: No Descrizione: defined

COGNOME	Rosa	NOME	Giancarlo	
RUOLO:	Referente Informatico			
TELEFONO LAVORO		CELLULARE		MAIL LAVORO informatico@ss.camcom.it
UFFICIO COMPETENTE				
COGNOME	Sini	NOME	Gavino	
RUOLO:	Presidente - Rappresentante Legale			
TELEFONO LAVORO		CELLULARE		MAIL LAVORO gavino.sini@ss.camcom.it
UFFICIO COMPETENTE				
COGNOME	Tanca	NOME	Massimo	
RUOLO:	Referente Informatico			
TELEFONO LAVORO		CELLULARE		MAIL LAVORO massimo.tanca@infocamere.it

**UFFICIO
COMPETENTE**

Team: Ruoli di responsabilità e competenza

Descrizione:: No Descrizione: defined

COGNOME	Tiloca	NOME	Franca		
RUOLO:	Responsabile Continuità Operativa				
TELEFONO LAVORO		CELLULARE		MAIL LAVORO	francesca.tilocca@ss.ca mcom.it
UFFICIO COMPETENTE					

10 Fornitori

Exported On: 8 Jan 2018

NOME FORNITORE	Infocamere SCpA		
DESCRIZIONE	La Società di Informatica delle Camere di Commercio Italiane		
SEDE	Infocamere S.C.p A. Sede Operativa		
INDIRIZZO - SEDE	C. so Uniti, 14		
CITTÀ - SEDE	Padova	CODICE POSTALE - SEDE	35127
TELEFONO - SEDE	049 8089610		
INFORMAZIONI AGGIUNTIVE	Centralino sede Padova di Infocamere: 049.8089610 foritore dei servizi attribuiti ad Infocamere in Elenco Servizi_Generalita' 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.		

NOME FORNITORE	UNO SRL		
DESCRIZIONE	Società a responsabilità limitata		
SEDE	UNO Srl		

INDIRIZZO - SEDE	VIA DIAZ 20		
CITTÀ - SEDE	SASSARI	CODICE POSTALE - SEDE	07100
TELEFONO - SEDE			
INFORMAZIONI AGGIUNTIVE	Supporto del sito internet camerale con hosting su server dedicati, analisi e statistiche e ricalibrazione della strategia di posizionamento, assistenza telefonica, via mail e via chat attraverso apposita sezione del back office, 100 crediti per il download e l'utilizzo di immagini 123rf.com.		

11 Riferimenti normativi

Exported On: 8 Jan 2018

Tipo: Riferimenti

TERMINE / ACRONIMO	Norma - ISO 22301:2012
DEFINIZIONE VITAL RECORD	"Societal Security - Business continuity management system - Requirements"
DEFINIZIONE	
TERMINE / ACRONIMO	Norma ISO/IEC 24762:2008
DEFINIZIONE VITAL RECORD	"Information technology - Security techniques - Guidelines for information and communication technology disaster recovery continuity"
DEFINIZIONE	
TERMINE / ACRONIMO	Norma ISO/IEC 27031:2011

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

DEFINIZIONE	
--------------------	--

Tipo: Riferimenti

TERMINE / ACRONIMO	Piano AGID
---------------------------	------------

DEFINIZIONE VITAL RECORD	Piano AGID_linea guida PCO
---------------------------------	----------------------------

DEFINIZIONE	Le "LINEE GUIDA PER IL DISASTER RECOVERY DELLE PUBBLICHE AMMINISTRAZIONI" sono disponibili al sito: http://www.agid.gov.it/sites/default/files/linee_guida/linee-guida-dr.pdf
--------------------	--

TERMINE / ACRONIMO	Piano di Protezione Civile
---------------------------	----------------------------

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

DEFINIZIONE	
--------------------	--

12 Elenco Personale nel Piano

Exported On: 8 Jan 2018

COGNOME	NOME	TELEFONO LAVORO	CELLULARE
Crobu	Luca		
Esposito	Pietro		
Nughes	Leonardo		
Rosa	Giancarlo		
Sini	Gavino		
Tanca	Massimo		
Tiloca	Franca		