



CITTÀ DI BELGIOIOSO

Provincia di Pavia

C.F. 00397220187 Cod. F.E. UFVUFW
Codice Istat 018013 - Codice Catastale A741

Municipio: Via Garibaldi, 64 27011 Belgioioso (PV)

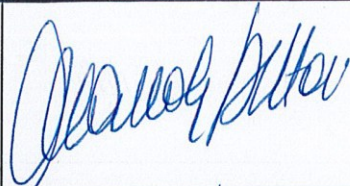
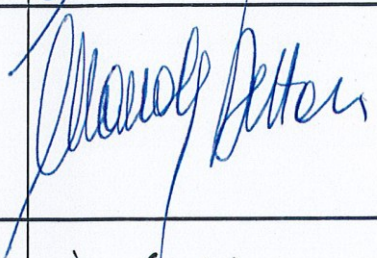
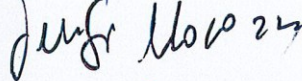
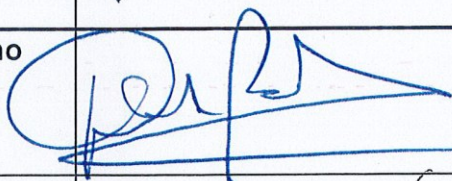
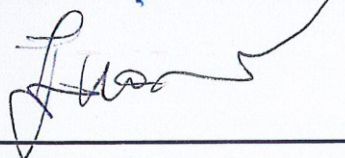
Tel. 0382-97841

PEC: comune.belgioioso@pec.regione.lombardia.it - www.comune.belgioioso.pv.it

Piano di Continuità Operativa e Disaster Recovery ICT



Approvazione	Data	Elenco di distribuzione	Sommario Modifiche
Versione 5.0	Marzo 2025	v. paragrafo	
Versione 5.1	Febbraio 2026	v. paragrafo	

FIRME			
	Unità/Ruolo	Nominativo	Firma
PREPARATO DA:	Resp. del settore ICT	Dr. Manola Dettori	
CONTROLLATO DA:	Resp. Transizione Digitale	Dr. Manola Dettori	
APPROVATO DA:	Assessore	Luigi Marozzi	
APPROVATO DA:	Segretario	Dr. Daniele Bellomo	
AUTORIZZATO DA:	Sindaco	Prof. Fabio Zucca	

ELENCO DI DISTRIBUZIONE:

Nominativo	
Segretario	Dr. Daniele Bellomo
Responsabile Continuità operativa	Dr. Manola Dettori
Responsabile Transazione Digitale	Dr. Manola Dettori

REGISTRO DELLE MODIFICHE		
EDIZIONE	SINTESI DELLA MODIFICA	DATA
2.1	Aggiornamento sistema di backup e procedure di recovery sito secondario	01.03.2016
2.1	Adeguamento normativa UE NI2	01.02.2026

Sommario

1	Obiettivi generali	8
1.1	Obiettivo del Piano di Continuità Operativa ICT	9
1.2	Destinatari	10
1.3	I servizi in ambito nello SFT	10
1.4	Variazioni eventuali nel numero dei servizi e relative criticità	12
1.5	Matrice servizi/organizzazione (responsabilità)	13
1.6	Matrice servizi/infrastruttura tecnologica	13
2	Predisposizione all'emergenza	17
2.1	La struttura organizzativa	17
2.2	Comitato di crisi ICT	17
2.3	Responsabile della Continuità Operativa ICT	17
2.4	Strutture tecniche	17
2.5	Composizione, ruoli, procedure operative	19
2.6	Gestione delle reperibilità	19
3	Soluzione di continuità-Ricognizione sulle infrastrutture ICT	21
3.1	Procedura di emergenza	21
3.2	Procedure di avviamento del sito secondario	29
3.3	Ripristino del sito di produzione	34
4	Formazione	38
5	Verifica/test del piano	39
5.1	Obiettivi e strategie di test	39
5.2	Procedure di test e verifica	39
6	Manutenzione del piano	41
6.1	Aggiornamento del piano	41

1 Obiettivi generali

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 ed i compiti che spettano alle Pubbliche Amministrazioni, all'Agenzia per l'Italia Digitale (AID) e al Ministro per la pubblica amministrazione e l'innovazione, ai fini dell'attuazione della continuità operativa, disponendo come segue::

"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 ed 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 ed 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 ed organizzative per garantire il funzionamento dei centri di elaborazione dati e delle procedure informatiche rilevanti in siti alternativi a quelli di produzione.

AID, 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.

1.1 Obiettivo del Piano di Continuità Operativa ICT

L'obiettivo di questo Piano di Continuità Operativa ICT (nel seguito, semplicemente PCO) è quello di definire organizzazione, procedure, mezzi tecnici che permettano all'Amministrazione di ripristinare, in caso di interruzioni di qualunque natura, i propri servizi; il PCO ICT ha la finalità di:

- Gestire un completo e definitivo ripristino dell'operatività in caso di disastro;
- Reagire agli eventi nel modo più tempestivo possibile;
- Stabilire un flusso di comunicazione efficiente in tempi brevissimi in caso di emergenza

Si sottolinea che il Piano oggetto di questo documento si differenzia nelle finalità da altri Piani richiesti dalle normative vigenti, quali:

Piano di Protezione Civile, secondo Ordinanza del Presidente del Consiglio dei Ministri del 28 agosto 2007, n. 3606,

Piano di Emergenza, secondo DL 81/2008.

Si precisa, però, che il Piano è stato comunque verificato come coerente con le suddette normative.

Benché il presente Piano rappresenti una specifica realizzazione nel contesto di quanto previsto dall'articolo 50-bis del CAD e non sia, quindi, direttamente riconducibile a un preciso standard, sono norme internazionali di riferimento le seguenti:

ISO 22301:2012 ("Societal security – Business continuity management systems – Requirements")

ISO/IEC 27031:2011 ("Information technology -- Security techniques -- Guidelines for information and communication technology readiness for business continuity")

ISO/IEC 24762:2008 ("Information technology -- Security techniques -- Guidelines for information and communications technology disaster recovery services")

NORMATIVA UE NIS2 (Network and Information Security Directive 2)

Introduzione

La direttiva NIS2 (Network and Information Security Directive 2) rappresenta l'evoluzione del quadro normativo europeo in materia di sicurezza delle reti e dei sistemi informativi, con l'obiettivo di rafforzare la resilienza cibernetica degli Stati membri e dei soggetti pubblici e privati che erogano servizi essenziali o importanti. Per quanto riguarda la Pubblica Amministrazione (PA), la normativa incide in modo significativo sulla continuità operativa dei sistemi informativi, considerata elemento imprescindibile per garantire la disponibilità, l'integrità e la riservatezza dei servizi pubblici digitali.

La NIS2 si inserisce nel contesto delle politiche di sicurezza dell'Unione Europea e, in Italia, trova attuazione operativa anche attraverso il coordinamento dell'Agenzia per la Cybersicurezza Nazionale, che svolge funzioni di indirizzo, monitoraggio e supporto per i soggetti della PA.

Di seguito si descrivono gli obiettivi principali della normativa NIS2 con riferimento specifico alla continuità operativa dei sistemi informativi della Pubblica Amministrazione.

1. Rafforzamento della resilienza operativa dei sistemi informativi

Un primo obiettivo fondamentale della NIS2 è assicurare la **resilienza dei sistemi informativi delle amministrazioni pubbliche, intesa come capacità di prevenire, resistere e recuperare da incidenti informatici che possano compromettere l'erogazione dei servizi.**

La direttiva impone l'adozione di misure tecniche e organizzative adeguate e proporzionate ai rischi, tra cui:

gestione del rischio informatico;

politiche di sicurezza documentate;

protezione delle infrastrutture critiche;

meccanismi di backup e ripristino.

Tali misure mirano a garantire che, anche in presenza di attacchi cyber o malfunzionamenti, i sistemi informativi della PA possano continuare a funzionare o essere rapidamente ripristinati, evitando interruzioni prolungate dei servizi essenziali (es. anagrafe, sanità digitale, servizi tributari, piattaforme di pagamento).

2. Introduzione di un approccio strutturato alla gestione del rischio

La continuità operativa è strettamente connessa alla gestione del rischio ICT. La NIS2 richiede alle PA di adottare un approccio sistemico e continuo alla valutazione e mitigazione dei rischi, attraverso:

analisi periodiche delle vulnerabilità;

valutazioni d'impatto sugli asset critici;

piani di trattamento del rischio;

aggiornamento costante delle misure di sicurezza.

L'obiettivo è superare una logica reattiva e promuovere una gestione proattiva della sicurezza, che consenta di prevenire gli incidenti anziché limitarne solo gli effetti. In questo modo, la continuità operativa diventa il risultato di un processo strutturato e continuo di governance della sicurezza.

3. Obbligo di piani di continuità operativa e disaster recovery

Uno dei cardini della NIS2 riguarda l'obbligo di predisporre e mantenere aggiornati:

piani di continuità operativa (Business Continuity Plan);

piani di disaster recovery;

procedure di ripristino dei servizi critici.

Questi strumenti devono essere testati regolarmente tramite esercitazioni e simulazioni di incidenti cyber, al fine di verificare la reale capacità dell'amministrazione di garantire la continuità dei servizi in scenari di crisi.

L'obiettivo è assicurare che, in caso di attacco informatico o guasto grave, i sistemi informativi possano essere ripristinati entro tempi compatibili con i livelli di servizio richiesti, riducendo l'impatto su cittadini e imprese.

4. Miglioramento delle capacità di rilevazione e risposta agli incidenti

La continuità operativa non dipende solo dalla prevenzione, ma anche dalla capacità di individuare e gestire rapidamente gli incidenti di sicurezza. La NIS2 introduce obblighi stringenti in materia di:

monitoraggio continuo dei sistemi;

rilevazione tempestiva delle anomalie;

gestione strutturata degli incidenti;

notifica obbligatoria alle autorità competenti.

Per la PA, ciò comporta l'adozione di sistemi di Security Operations (SOC), log management e strumenti di incident response, che permettano di contenere gli effetti di un attacco e di garantire la rapida ripresa delle attività operative.

5. Rafforzamento della governance e delle responsabilità dirigenziali

Un ulteriore obiettivo della direttiva è quello di rafforzare la governance della sicurezza informatica all'interno delle amministrazioni pubbliche. La NIS2 attribuisce precise responsabilità agli organi di vertice, i quali devono:

approvare le politiche di sicurezza;

supervisionare l'attuazione delle misure di continuità operativa;

garantire adeguate risorse organizzative e tecnologiche.

Questo approccio mira a integrare la sicurezza e la continuità operativa nei processi decisionali strategici della PA, evitando che tali aspetti siano considerati esclusivamente questioni tecniche.

6. Sicurezza della supply chain e continuità dei servizi digitali

La NIS2 estende l'attenzione alla sicurezza dell'intera catena di fornitura ICT. Le amministrazioni pubbliche dipendono sempre più da fornitori esterni (cloud provider, software house, servizi gestiti); eventuali vulnerabilità di questi soggetti possono compromettere la continuità operativa dei sistemi pubblici.

La direttiva richiede quindi:

valutazioni di sicurezza dei fornitori;

clausole contrattuali specifiche sulla continuità del servizio;

controllo dei rischi derivanti da terze parti.

L'obiettivo è evitare che interruzioni o incidenti presso fornitori critici possano bloccare servizi pubblici digitali essenziali.

7. Cooperazione istituzionale e condivisione delle informazioni

La continuità operativa della PA è favorita anche dal rafforzamento della cooperazione tra amministrazioni e autorità nazionali ed europee. La NIS2 promuove:

scambio di informazioni su minacce e vulnerabilità;

coordinamento nella gestione degli incidenti su larga scala;

partecipazione a reti di risposta alle crisi cyber.

Questo approccio collaborativo consente una risposta più efficace e coordinata agli eventi che potrebbero compromettere il funzionamento dei sistemi informativi pubblici.

Conclusioni

In sintesi, gli obiettivi principali della normativa NIS2 in relazione alla continuità operativa dei sistemi informativi della Pubblica Amministrazione possono essere ricondotti a cinque direttrici fondamentali:

Rafforzare la resilienza dei sistemi informativi e la capacità di garantire l'erogazione continua dei servizi pubblici digitali.

Introdurre una **gestione strutturata e proattiva del rischio** informatico.

Rendere obbligatori **piani di continuità operativa e disaster recovery** testati e aggiornati.

Migliorare le **capacità di rilevazione, risposta e recupero** dagli incidenti cyber.

Integrare la sicurezza e la continuità operativa nella governance strategica della PA, includendo anche la gestione dei rischi della supply chain.

La direttiva NIS2 segna quindi un passaggio da un approccio reattivo a uno **preventivo e sistemico**, ponendo la continuità operativa dei sistemi informativi al centro della trasformazione digitale sicura della Pubblica Amministrazione.

1.2 Destinatari

Destinatari del Piano di Continuità Operativa ICT sono:

Il Sindaco ed il Segretario dell'Ente

il responsabile della CO ICT dell'ente, così come indicato nelle "Linee guida per il DR delle PA" emesso dall'Agenzia per l'Italia Digitale il 26 novembre 2011;

il responsabile della transizione digitale;

il responsabile della sicurezza dei luoghi di lavoro dell'Ente;

il personale dell'Amministrazione di qualunque tipologia (fruitore o gestore) direttamente coinvolto nell'IT dell'Amministrazione;

la comunità di riferimento territoriale e sociale (cittadini e imprese) dell'Amministrazione;

le organizzazioni e/o istituzioni che interagiscono con l'Amministrazione in modalità informatiche;

tutti i fornitori, a qualunque titolo, di attività di supporto informatico.

1.3 I servizi in ambito nello SFT

I servizi in ambito identificati nello SFT CON I RELATIVI LIVELLI (Tier) di criticità sono stati seguenti:

Servizio / classe servizi	Classe criticità	Sol. Tecnologica minima da autovalutazione	Soluzione tecnica individuata	Soluzione già presente	RPO	RTO
Classe 1A	Media	Tier 3	Soluzione A	Backup linea F.O. via accesso 5G al cloud	8 Ore	24 Ore
Classe 2A	Media	Tier 2	Soluzione A	Backup linea F.O. via accesso 5G al cloud	8 Ore	24 Ore
Classe 2B	Media	Tier 2	Soluzione A	Backup linea F.O. via	8 Ore	24 Ore

Classe 2C	Media	Tier 2	Soluzione B	Backup linea F.O. via accesso 5G al cloud	8 Ore	24 Ore
Classe 3A	Media	Tier 2	Soluzione A	Backup linea F.O. via accesso 5G al cloud	8 Ore	24 Ore

1.4 Variazioni eventuali nel numero dei servizi e relative criticità.

Servizio / classe servizi	Classe criticità	Sol. Tecnologica minima da autovalutazione	Soluzione tecnica individuata	Soluzione già presente	RPO	RTO
Classe 1A	Media	Tier 3	Soluzione A	Backup linea F.O. via accesso 5G al cloud	8 Ore	24 Ore
Classe 2A	Media	Tier 2	Soluzione A	Backup linea F.O. via accesso 5G al cloud	8 Ore	24 Ore
Classe 2B	Media	Tier 2	Soluzione A	Backup linea F.O. via accesso 5G al cloud	8 Ore	24 Ore
Classe 2C	Media	Tier 2	Soluzione B	Backup linea F.O. via accesso 5G al cloud	8 Ore	24 Ore
Classe 3A	Media	Tier 2	Soluzione A	Backup linea F.O. via accesso 5G al cloud	8 Ore	24 Ore

1.5 Matrice servizi/organizzazione (responsabilità)

Classe di Servizi	Servizio	Descrizione servizio	Tipologia di Utenza
Classe 1A	Servizio SEG_1	Gestione atti amministrativi	Eterogenea
Classe 1A	Servizio RAG_1	Gestione finanziaria-impegni e mandati	Eterogenea
Classe 1A	Servizio SOC_1	Servizi sociali - Attività relativa ai trattamenti sanitari obbligatori (T.S.O.) ed all'assistenza sanitaria obbligatoria (A.S.O.)	Aziende/cittadini
Classe 1A	Servizio SOC_1	Servizi sociali - Attività relativa all'assistenza domiciliare	Aziende/cittadini
Classe 1A	Servizio WEB	Sito web istituzionale	Eterogenea

Classe di Servizi	Servizio	Descrizione servizio	Tipologia di Utenza
Classe 2A	Servizio PERS_1	Personale - Gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune – attività relativa al riconoscimento di benefici connessi all'invalidità civile e all'invalidità derivante da cause di servizio, nonché da riconoscimento di inabilità a svolgere attività lavorativa	Utente Interno
Classe 2A	Servizio SOC_2	Servizi sociali - Attività relativa all'assistenza scolastica ai portatori di handicap o con disagio psico-sociale	Aziende/cittadini
Classe 2A	Servizio SOC_2	Servizi sociali - Attività relativa alle richieste di ricovero o inserimento in Istituti, Case di cura, Case di riposo, ecc.	Aziende/cittadini
Classe 2A	Servizio SOC_2	Servizi sociali - Attività ricreative per la promozione del benessere della persona e della comunità, per il sostegno dei progetti di vita delle persone e delle famiglie e per la rimozione del disagio sociale	Aziende/cittadini
Classe 2A	Servizio SOC_2	Servizi sociali - Attività relativa alla valutazione dei requisiti necessari per la concessione di contributi, ricoveri in istituti convenzionati o soggiorno estivo (per soggetti audiolesi, non vedenti, pluriminorati o gravi disabili o con disagi psico-sociali)	Aziende/cittadini
Classe 2A	Servizio SOC_2	Servizi sociali - Attività relativa all'integrazione sociale ed all'istruzione del portatore di handicap e di altri soggetti che versano in condizioni di disagio sociale (centro diurno, centro socio educativo, ludoteca, ecc.)	Aziende/cittadini

Classe 2A	Servizio SOC_2	Servizi sociali - Attività di sostegno delle persone bisognose o non autosufficienti in materia di servizio pubblico di trasporto	Aziende/cittadini
Classe 2A	Servizio SOC_2	Servizi sociali - Attività relativa alla prevenzione ed al sostegno alle persone tossicodipendenti ed alle loro famiglie tramite centri di ascolto (per sostegno) e centri documentali (per prevenzione)	Aziende/cittadini
Classe 2A	Servizio SOC_2	Servizi sociali - Attività relative alla concessione di benefici economici, ivi comprese le assegnazioni di alloggi di edilizia residenziale pubblica e le esenzioni di carattere tributario	Aziende/cittadini
Classe 2A	Servizio SOC_2	Istruzione e cultura - Attività relativa alla gestione degli asili nido comunali e dei servizi per l'infanzia e delle scuole materne elementari e medie	Aziende/cittadini
Classe 2A	Servizio SOC_2	Istruzione e cultura - Attività di formazione ed in favore del diritto allo studio	Aziende/cittadini
Classe 2A	Servizio SOC_1	Istruzione e cultura - Gestione delle biblioteche e dei centri di documentazione	Aziende/cittadini
Classe 2A	Servizio PM	Polizia municipale - Attività relativa all'infortunistica stradale	Aziende/cittadini
Classe 2A	Servizio PM	Polizia municipale - Gestione delle procedure sanzionatorie	Aziende/cittadini
Classe 2A	Servizio PM	Polizia municipale - Attività di polizia annonaria, commerciale ed amministrativa	Aziende/cittadini
Classe 2A	Servizio PM	Polizia municipale - Attività di vigilanza edilizia, in materia di ambiente e sanità, nonché di polizia mortuaria	Aziende/cittadini
Classe 2A	Servizio PM	Rilascio delle licenze per il commercio, il pubblico esercizio, l'artigianato e la pubblica sicurezza	Eterogenea
Classe 2A	Servizio SEG_2	Attività politica, di indirizzo e di controllo, sindacato ispettivo e documentazione dell'attività istituzionale degli organi comunali	Utente Interno
Classe 2A	Servizio SEG_2	Attività riguardante gli istituti di democrazia diretta	Eterogenea
Classe 2A	Servizio PRC	Protezione civile	Aziende/cittadini
Classe 2B	Servizio	Albo Pretorio Informatico	Eterogenea

Classe 2C	Servizio SUAP	Sportello unico attività produttive	Eterogenea
-----------	---------------	-------------------------------------	------------

Classe di Servizi	Servizio	Descrizione servizio	Tipologia di Utente
Classe 3A	Servizio RAG_2	Gestione economale	Eterogenea
Classe 3A	Servizio RAG_2	Gestione finanziaria-bilancio	Eterogenea
Classe 3A	Servizio PM_2	Polizia municipale - Attività relativa al rilascio di permessi per invalidi	Aziende/cittadini
Classe 3A	Servizio SEG_3	Avvocatura - Attività relative alla consulenza giuridica, al patrocinio, alla difesa in giudizio dell'amministrazione, nonché alla consulenza e copertura assicurativa in caso di responsabilità civile verso terzi dell'amministrazione	Utente Interno
Classe 3A	Servizio PERS_1	Politiche del lavoro - Gestione delle attività relative all'incontro domanda/offerta di lavoro, comprese quelle relative alla formazione professionale	Aziende/cittadini
Classe 3A	Servizi SOC_3	Attività ricreative, promozione della cultura e dello sport ed occupazioni di suolo pubblico	Eterogenea
Classe 3A	Servizi SOC_3	Servizi sociali - Attività relativa ai servizi di sostegno e sostituzione al nucleo familiare e alle pratiche di affido e di adozione dei minori	Aziende/cittadini

1.6 Matrice servizi/infrastruttura tecnologica

Indice di tecnologia	"A"	"B"	"C"	LDS (orario disponibilità)
Indice di priorità di ripristino	Gestione in Cloud	Gestione in Cloud	Gestione in Cloud	
"1" Servizi ad alto impatto, di immediata necessità, la cui disponibilità deve essere ripristinata rapidamente al fine di gestire l'emergenza stessa	Classe 1A	Classe 1B	Classe 1C	24h - CLOUD
"2" Servizi ad alto impatto, non necessari alla immediata gestione dell'emergenza, il cui ripristino avviene successivamente ai servizi "1"	Classe 2A	Classe 2B	Classe 2C	24h - CLOUD

"3" Servizi ad impatto medio/basso, non necessari alla gestione dell'emergenza, il cui ripristino può avvenire in un tempo di più giorni o settimane	Classe 3A	Classe 3B	Classe 3C	24h - CLOUD
--	------------------	------------------	------------------	--------------------

2 Predisposizione all'emergenza

2.1 La struttura organizzativa

La struttura organizzativa che l'Amministrazione ha predisposto presenta la seguente articolazione funzionale:

- 1) **Il Comitato di gestione della crisi**, le cui funzioni sono quelle stabilite dalla linee guida sulla CO.
- 2) **I dipendenti dell'ente, inseriti in un apposito elenco (Comitato Gestione dell'Emergenza)**, che devono partecipare alle attività di protezione, salvataggio e ripristino delle informazioni e dei dati in condizioni di emergenza, riportando le azioni che devono essere poste in carico a ciascuno di loro, i relativi interlocutori e le modalità da rispettare.

2.2 Comitato di crisi ICT

Le funzioni di questo organismo sono quelle stabilite dalla linee guida sulla CO. La sua composizione è formata dai seguenti soggetti:

Segretario Comunale
Responsabile della Transizione digitale
Responsabile della sicurezza ex D.Lgs. 81/08
Referenti aziende fornitrici (con funzioni di supporto al Comitato)

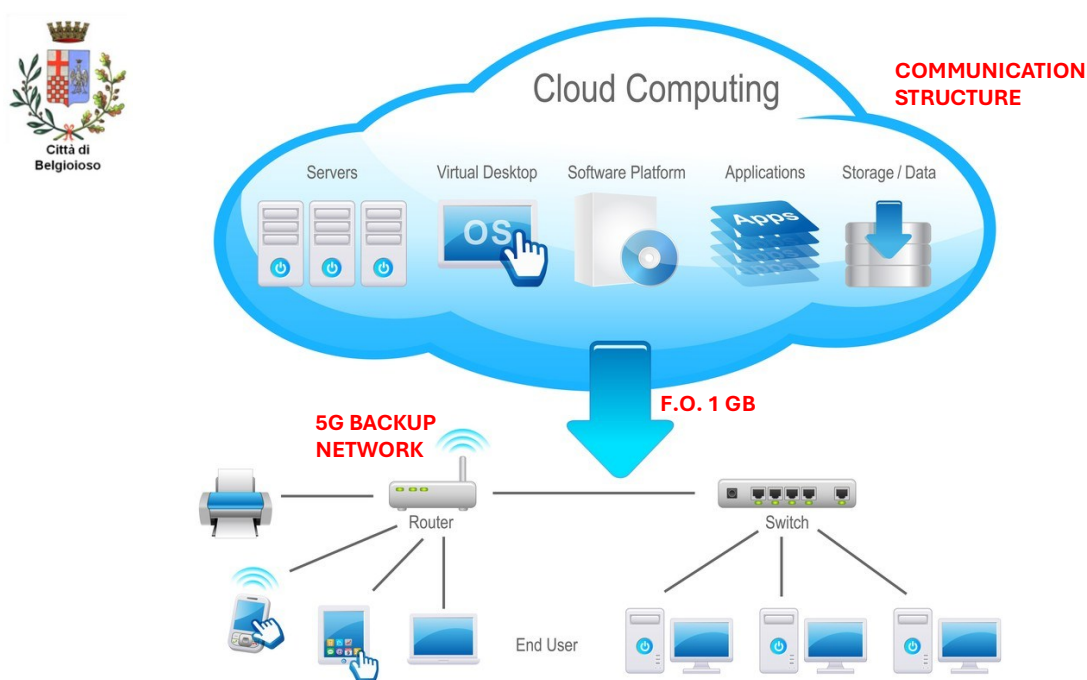
2.3 Responsabile della Continuità Operativa ICT

Svolge le funzioni il dr.ssa Manola Dettori nel ruolo di responsabile della UO

2.4 Strutture tecniche

SITO PRIMARIO – SEDE MUNICIPALE

SITO PRIMARIO (Infrastruttura ICT Amministrazione Comunale)



La descrizione della piattaforma tecnologica che viene impiegata per l'esercizio del sito primario viene riportata di seguito che riporta l'architettura e le configurazioni degli apparati di elaborazione operanti presso l'Ente nonché la dotazione di applicazioni informatiche e delle risorse informative (basi di dati) che caratterizzano il sistema informativo.

SITO SECONDARIO - CLOUD

Il Centro Backup Remoto (CBR o Sito Secondario) è composto essenzialmente dalle risorse messe a disposizione dal cloud.

Il supporto tecnico del Centro backup Remoto - CBR mantiene apparecchiature sempre attive, condivise e non ad uso esclusivo di un singolo ente. L'Ente ha uno spazio storage riservato per la replica di tutti i dati. Sono presenti macchine virtuali su cui installare in caso di necessità gli applicativi gestionali dell'ente e delle postazione client erogate in modalità terminal server raggiungibili dai dipendenti dell'ente tramite linea internet.

Per l'implementazione dei sistemi utilizza la piattaforma Cloud: un sistema operativo cloud che controlla un insieme di risorse computazionali, storage e di rete presenti nel data center in forma virtualizzata, tutte gestite utilizzando una dashboard che fornisce il controllo completo all'amministratore e inoltre, attraverso l'utilizzo di un'interfaccia web, offre all'utente funzionalità di self-service provisioning.

La scelta della piattaforma di virtualizzazione è di tipo misto per consentire la gestione dei diversi ambienti e semplificare ulteriormente l'integrazione. Il sistema consente di virtualizzare anche i desktop (o almeno le postazioni più critiche) per arrivare a una amministrazione il più possibile ICT free. In termini di economicità la virtualizzazione permette topologicamente di integrare le piattaforme delle cinque aggregazioni in un'unica piattaforma logica facilitandone e ottimizzandone la gestione.

Nella configurazione attuale il Nodo Primario è costituito dai seguenti ambienti virtuali:

- Procedure applicative e gestionali
- Produttività individuali e office automation
- Portali istituzionali
- Sistema di messaggistica integrata

2.5 Composizione, ruoli, procedure operative

I soggetti coinvolti sono i seguenti:

Ufficio	Ruolo	Descrizione ruolo	Figura Professionale	Responsabilità
Information Technology	Responsabile Sistemi Informativi	Coordina e verifica la struttura tecnica legata alla gestione delle informazioni, alla corretta configurazione e gestione dell'hardware	Istruttore Direttivo	Responsabile dell'attuazione del piano di DR
Segretario Comunale	Segretario Comunale	Coordina i Responsabili di settore o Area	Segretario Comunale	Coordina i Responsabili di Servizio e Impartisce idonei obiettivi per la gestione della Crisi
Ufficio Servizi Finanziari ed Economale	Responsabile/dirigente Settore	Gestione delle Risorse finanziarie per fronteggiare la Crisi e rientrare dall'emergenza	Istruttore Direttivo	Responsabilità: Adeguare le disponibilità di bilancio per far fronte agli oneri della CO ICT
Ufficio Tecnico	Responsabile/dirigente Settore	Gestione delle infrastrutture logistiche	Dirigente/Istruttore Direttivo	Responsabile delle strutture logistiche impianti e cablaggi. Verifica la corretta erogazione delle forniture elettriche
Tecnici Centro Cloud	Direttore Responsabile centro tecnico presso cloud	Coordina i tecnici nell'attivazione del Cloud, coordina le procedure e tempi per il rientro dell'emergenza	Direttore	Responsabile delle operazioni tecniche e di gestione del sito secondario dall'attivazione al suo rientro

2.6 Gestione delle reperibilità

Reperibilità del comitato gestione di emergenza e dei soggetti coinvolti nelle operazioni di ripristino dei servizi.

Il regolamento dell'ente sulla CO prevede l'estensione dell'istituto della reperibilità, nella situazione di annuncio delle condizioni di emergenza, a tutti i dipendenti richiamati nell'elenco di cui al precedente paragrafo. Tale istituto, su disposizione del Comitato di crisi, può essere esteso anche ad altri dipendenti o collaboratori.

Nei rapporti con i fornitori esterni di servizi ICT interessati all'esercizio delle procedure applicative e dei servizi ICT viene prevista una integrazione contrattuale con la quale si dispongono termini e condizioni dell'intervento di supporto per la gestione dell'emergenza ICT.

3 Soluzione di continuità-Ricognizione sulle infrastrutture ICT dell'Ente

3.1 Procedura di emergenza

3.1.1 Criteri di sicurezza e Valutazione dell'emergenza

La valutazione dell'emergenza è classificata in base alla criticità e livello di impatto sull'amministrazione

CRITICITÀ DI LIVELLO 1	Le applicazioni che rientrano in questa classificazione, e che sono di seguito elencate, influenzano direttamente l'Amministrazione ed eventuali malfunzionamenti possono portare significativi danni di immagine, economici e legali.
CRITICITÀ DI LIVELLO 2	Le applicazioni che rientrano in questa classificazione, e che sono di seguito elencate, influenzano direttamente il buon andamento dell'ente, ma non sono servizi critici che possono comportare un danno alla sicurezza o salute pubblica.
CRITICITÀ DI LIVELLO 3	Le applicazioni che rientrano in questa classificazione, e che sono di seguito elencate, aiutano a far funzionare i processi interni dell'Amministrazione. In generale un periodo di fermo è recuperabile.

Nello Studio di Fattibilità Tecnica i servizi erogati sono stati suddivisi in tre classi distinte valutando principalmente la criticità dovuta alla garanzia di esistenza in vita priorità/urgenza nel ripristino del servizio previsto dalla normativa e dalla sensibilità e quantità dei dati trattati.

Alla “**classe 1**” appartengono tutti quei servizi indispensabili per far fronte a qualsiasi tipo di minaccia ed evento che comprometta i sistemi informativi ospitati nel sito primario dell'ente.

La “**classe 2**” raccoglie i servizi ad alto impatto, ma ripristinabili in tempi successivi rispetto alla gestione dell'emergenza. Anche per questa classe di servizi, si distinguono le 3 categorie in base alla tecnologia di impianto.

Alla “**classe 3**” vengono riportati tutti quei servizi che possono per loro natura essere ripristinati anche in più giorni/settimane, pur garantendo la continuità del servizio anche attraverso l'uso di procedure alternative

La classificazione ha prodotto il seguente risultato:

CLASSE 1

Classe di Servizi	Servizio	Descrizione servizio	Tipologia di Utenza
Classe 1A	Servizio SEG_1	Gestione atti amministrativi	Eterogenea
Classe 1A	Servizio RAG_1	Gestione finanziaria-impegni e mandati	Eterogenea
Classe 1A	Servizio SOC_1	Servizi sociali - Attività relativa ai trattamenti sanitari obbligatori (T.S.O.) ed all'assistenza sanitaria obbligatoria (A.S.O.)	Aziende/cittadini
Classe 1A	Servizio SOC_1	Servizi sociali - Attività relativa all'assistenza domiciliare	Aziende/cittadini
Classe 1A	Servizio WEB	Sito web istituzionale	Eterogenea

CLASSE 2

Classe di Servizi	Servizio	Descrizione servizio	Tipologia di Utenza
Classe 2A	Servizio PERS_1	Personale - Gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune – attività relativa al riconoscimento di benefici connessi all'invalidità civile e all'invalidità derivante da cause di servizio, nonché da riconoscimento di inabilità a svolgere attività lavorativa	Utente Interno
Classe 2A	Servizio SOC_2	Servizi sociali - Attività relativa all'assistenza scolastica ai portatori di handicap o con disagio psico-sociale	Aziende/cittadini
Classe 2A	Servizio SOC_2	Servizi sociali - Attività relativa alle richieste di ricovero o Inserimento in Istituti, Case di cura, Case di riposo, ecc.	Aziende/cittadini
Classe 2A	Servizio SOC_2	Servizi sociali - Attività ricreative per la promozione del benessere della persona e della comunità, per il sostegno dei progetti di vita delle persone e delle famiglie e per la rimozione del disagio sociale	Aziende/cittadini

Classe 2A	Servizio SOC_2	Servizi sociali - Attività relativa alla valutazione dei requisiti necessari per la concessione di contributi, ricoveri in istituti convenzionati o soggiorno estivo (per soggetti audiolesi, non vedenti, pluriminorati o gravi disabili o con disagi psico-sociali)	Aziende/cittadini
Classe 2A	Servizio SOC_2	Servizi sociali - Attività relativa all'integrazione sociale ed all'istruzione del portatore di handicap e di altri soggetti che versano in condizioni di disagio sociale (centro diurno, centro socio educativo, ludoteca, ecc.)	Aziende/cittadini
Classe 2A	Servizio SOC_2	Servizi sociali - Attività di sostegno delle persone bisognose o non autosufficienti in materia di servizio pubblico di trasporto	Aziende/cittadini
Classe 2A	Servizio SOC_2	Servizi sociali - Attività relativa alla prevenzione ed al sostegno alle persone tossicodipendenti ed alle loro famiglie tramite centri di ascolto (per sostegno) e centri documentali (per prevenzione)	Aziende/cittadini
Classe 2A	Servizio SOC_2	Servizi sociali - Attività relative alla concessione di benefici economici, ivi comprese le assegnazioni di alloggi di edilizia residenziale pubblica e le esenzioni di carattere tributario	Aziende/cittadini
Classe 2A	Servizio SOC_2	Istruzione e cultura - Attività relativa alla gestione degli asili nido comunali e dei servizi per l'infanzia e delle scuole materne elementari e medie	Aziende/cittadini
Classe 2A	Servizio SOC_2	Istruzione e cultura - Attività di formazione ed in favore del diritto allo studio	Aziende/cittadini
Classe 2A	Servizio SOC_1	Istruzione e cultura - Gestione delle biblioteche e dei centri di documentazione	Aziende/cittadini
Classe 2A	Servizio PM	Polizia municipale - Attività relativa all'infortunistica stradale	Aziende/cittadini
Classe 2A	Servizio PM	Polizia municipale - Gestione delle procedure sanzionatorie	Aziende/cittadini
Classe 2A	Servizio PM	Polizia municipale - Attività di polizia annonaria, commerciale ed amministrativa	Aziende/cittadini
Classe 2A	Servizio PM	Polizia municipale - Attività di vigilanza edilizia, in materia di ambiente e sanità, nonché di polizia mortuaria	Aziende/cittadini
Classe 2A	Servizio PM	Rilascio delle licenze per il commercio, il pubblico esercizio, l'artigianato e la pubblica sicurezza	Eterogenea

Classe 2A	Servizio SEG_2	Attività politica, di indirizzo e di controllo, sindacato ispettivo e documentazione dell'attività istituzionale degli organi comunali	Utente Interno
Classe 2A	Servizio SEG_2	Attività riguardante gli istituti di democrazia diretta	Eterogenea
Classe 2A	Servizio PRC	Protezione civile	Aziende/cittadini
Classe 2B	Servizio PROTO	Albo Pretorio Informatico	Eterogenea
Classe 2C	Servizio SUAP	Sportello unico attività produttive	Eterogenea

CLASSE 3

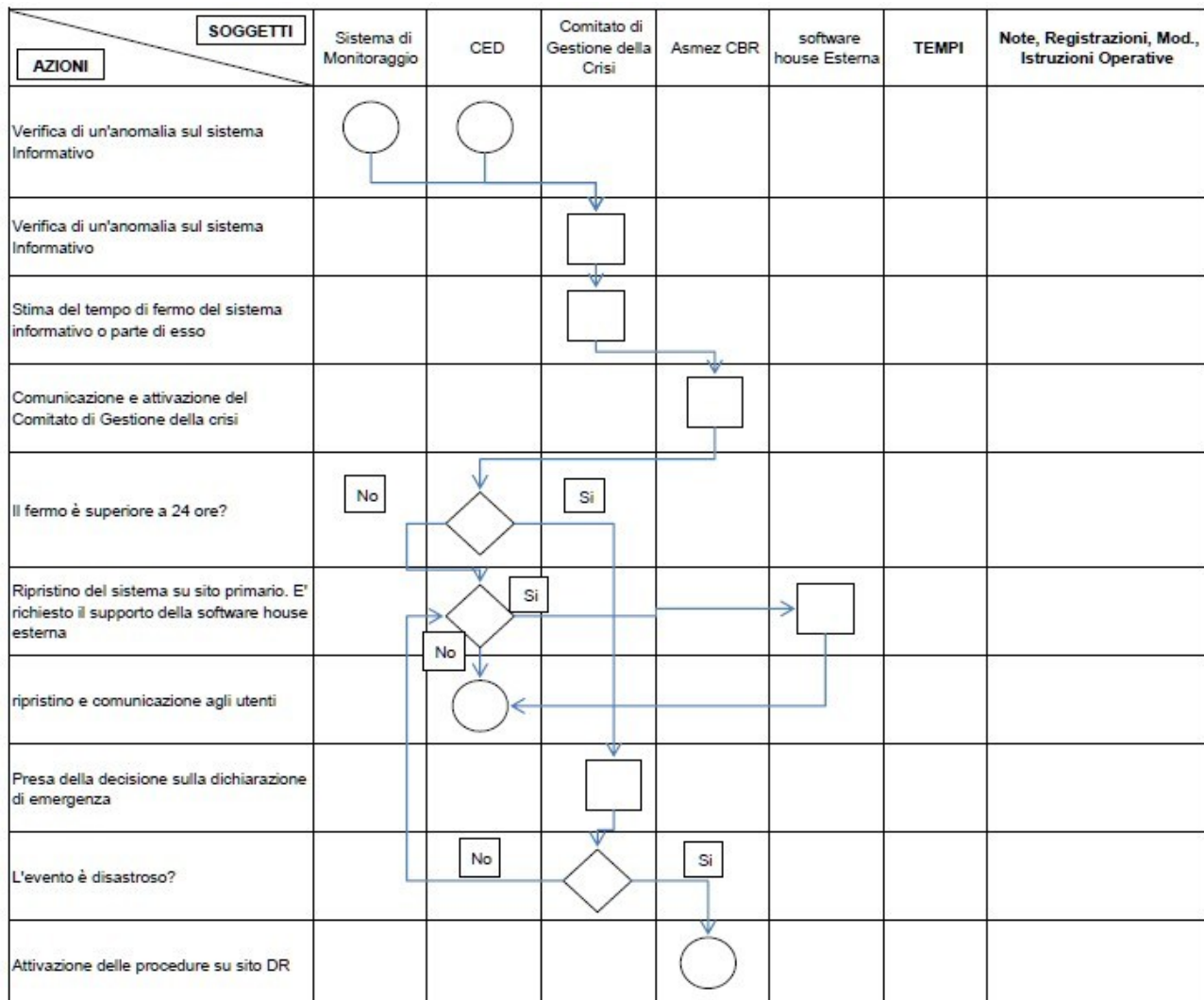
Classe di Servizi	Servizio	Descrizione servizio	Tipologia di Utenza
Classe 3A	Servizio RAG_2	Gestione economale	Eterogenea
Classe 3A	Servizio RAG_2	Gestione finanziaria-bilancio	Eterogenea
Classe 3A	Servizi SOC_3	Attività ricreative, promozione della cultura e dello sport ed occupazioni di suolo pubblico	Eterogenea
Classe 3A	Servizi SOC_3	Servizi sociali - Attività relativa ai servizi di sostegno e sostituzione al nucleo familiare e alle pratiche di affido e di adozione dei minori	Aziende/cittadini

3.1.2 Comunicazioni (Lista dei contatti in caso di disastro, modalità di contatto)

Le modalità di contatto per l'attivazione del piano sono definite contrattualmente fra Amministrazione e fornitori. Le procedure interne all'ente sono stabilite direttamente dal regolamento interno. I componenti del Comitato di gestione della crisi sono figure dirigenziali, quindi sempre reperibili, o comunque soggette a reperibilità attribuita con la nomina a Componente del Comitato di Gestione della Crisi. Il personale tecnico sarà contattato attraverso l'elenco dei tecnici reperibili.

3.1.3 Attivazione del piano di disaster recovery

La procedura di attivazione viene innescata ogni qualvolta si presenta una anomalia che può dar luogo ad una situazione di disastro descritta secondo la tabella riportata nel paragrafo 3.1.1. La sequenza delle comunicazioni prevede l'attivazione del processo di gestione concordato contrattualmente con il fornitore del servizio di AP Systems Cloud che prevede le seguenti fasi:



3.1.4 Scenari di emergenza applicabili e valutazione dei danni

Gli scenari individuati durante lo studio di fattibilità ci consentono di garantire dei livelli RTO e RPO per classi omogenee di servizi predefiniti nella classificazione riportata nel paragrafo 3.1.

La soluzione tecnologica scelta dall'amministrazione è definita secondo le linee guida pari al TIER 3, l'implementazione attuale della soluzione tecnica prevede dei tempi di RPO pari a quanto dichiarato nello studio di fattibilità mentre i tempi RTO sono maggiori.

Servizio/ Classe di Servizi	RTO	RPO
Classe 1	1 settimana in caso di distruzione della sede Municipale o impossibilità di accesso	1 giorno lavorativo
	2 giorni in caso di indisponibilità del network interno	
Classe 2		1 giorno lavorativo
Classe 3		1 giorno lavorativo

3.1.5 Procedure di acquisto in emergenza

Le procedure di acquisto in emergenza sono attivabili secondo quanto indicato nel regolamento interno dell'Ente. Tutti gli acquisti sono definiti e valutati dal Comitato di gestione della crisi

3.1.6 Documentazione delle attività svolte (reporting)

Tutte le attività di gestione e manutenzione del sistema effettuate dai tecnici delle aziende fornitrici mediante un dettagliato rapporto di intervento sottoscritto dall'amministrazione e dal direttore tecnico che certifica l'esito dell'intervento. I dati minimi riportati nel documento sono definiti nelle istruzioni operative della procedura di gestione e manutenzione e comprendono almeno: la data, l'ora, il luogo dello svolgimento del test, le figure che vi hanno partecipato, le prove svolte e l'esito.

In caso di insuccesso parziale o totale dei test, l'Amministrazione deve esaminare le problematiche emerse e attivare le azioni necessarie per la loro risoluzione.

In tal caso il verbale dei risultati dei test indicherà le azioni da intraprendere per la rimozione degli eventuali problemi riscontrati nel corso dei test unitamente alla persona o struttura incaricata di rimuoverli e alla scadenza prevista.

Tutti i verbali ovvero, il verbale di collaudo e quelli relativi ai test periodici svolti, fino al termine di validità della soluzione di continuità operativa e o del contratto che affida a AP Systems l'avvio, la realizzazione, la gestione e la manutenzione e verifica/test della soluzione, sono conservati dal AP Systems con le modalità di legge previste.

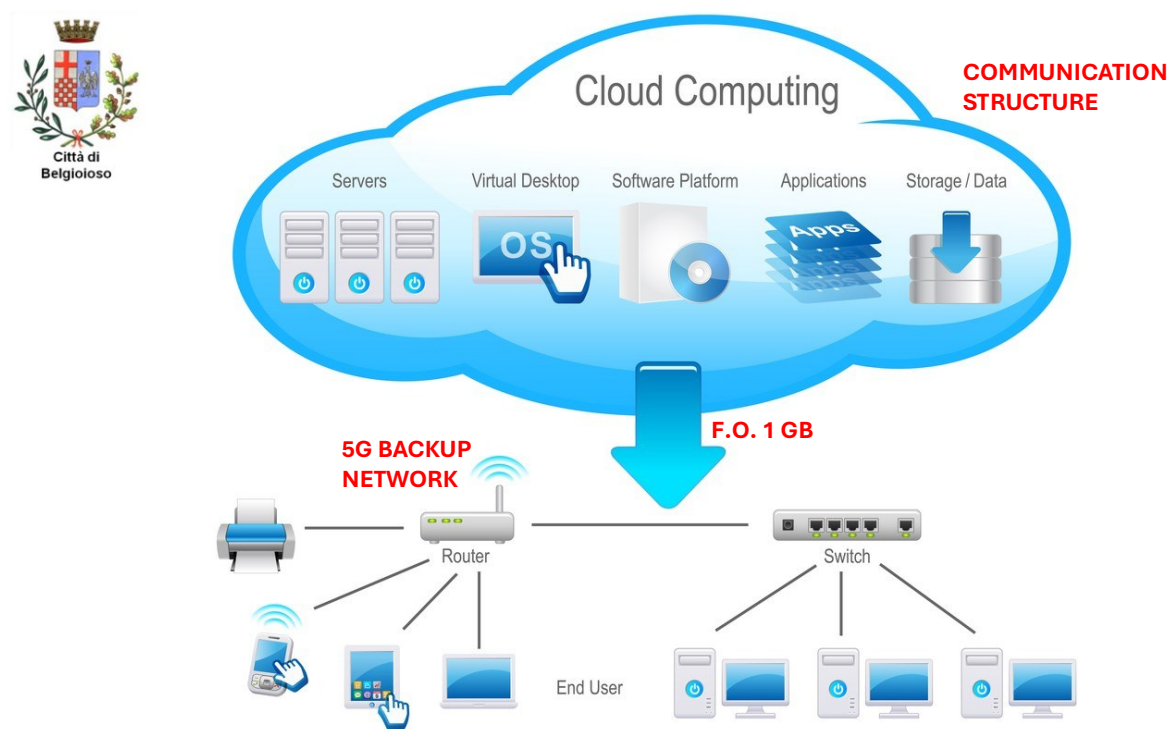
3.2 Procedure di avviamento del sito secondario

3.2.1 Preparazione del sito di disaster recovery

Il sistema cloud mantiene apparecchiature sempre attive, condivise e non ad uso esclusivo di un singolo ente. L'Ente ha uno spazio storage riservato per la replica di tutti i dati secondo delle logiche incrementali, inoltre sono presenti macchine virtuali per l'accesso in caso di necessità gli applicativi gestionali dell'ente e delle postazione client erogate in modalità terminal server raggiungibili dai dipendenti tramite internet.

Nel caso di una emergenza nel Sito Primario, per cui si renda necessario la ripartenza dei servizi dal CBR, tutte le apparecchiature ivi presenti e destinate all'utilizzo dell'Ente, sono attivate al fine di completare E' possibile attivare anche l'erogazione di una sola parte dei servizi danneggiati:

Schema logico dell'infrastruttura



Il ripristino dei servizi e degli archivi sono automatici interno del cloud, il quale si avvarrà del supporto delle software house che forniscono gli applicativi gestionali.

Tutte le operazioni sono gestibili e monitorate attraverso l'uso di un software che esegue giornalmente l'inoltro dei log sulle operazioni notturne di trasferimento dati dal sito primario al sito secondario. Il

Livelli di Servizio

RPO	1 giorno: Dati consolidati riferiti al giorno precedente rispetto all'evento disastroso
RTO	Questo indicatore vari a secondo dell'evento disastroso: - Riferito alla distruzione dell'intero sito primario è pari a 5 giorni lavorativi - Riferito alla perdita di parte di File o Archivi o parte delle banche dati gestionali è pari a 3 giorni lavorativi

Procedura Operativa P.PSDR.01

AZIONI SOGGETTI	Comitato di Gestione della Crisi	CED	TEMPI	Note, Registrazioni, Mod., Istruzioni Operative
Il Comitato di Gestione della Crisi vista la Situazione di Crisi sceglie di attivare il sito DR				
Verifica della situazione e validazione delle Azioni da intraprendere				Il Responsabile della CO dell'ente adotta le decisioni intraprese dal Comitato di Gestione della Crisi
Attivazione delle procedure di verifica di dati disponibili presso il CBR,				
Check della consistenza dei dati				
Procedura di ripristino dell'infrastruttura				Procedura Operativa P.PSDR.02
Procedura di ripristino della banche dati				Procedura Operativa P.PSDR.03
Procedura di ripristino delle applicazioni				Procedura Operativa P.PSDR.04
Procedura per la gestione dell'organizzazione logistica e coordinamento del personale				Procedura Operativa P.PSDR.05
check Finale del Sito DR Secondario				
Redazione e Sottoscrizione del Verbale ed inoltro al Comitato di Gestione della Crisi				
Configurazione delle Postazioni Client Presso L'Ente				
Ripresa della Attività Operative dal parte degli operatori dell'ente				

3.2.2 Procedura di ripristino dell'infrastruttura nel Sito Secondario

Il Sito Secondario dispone di un'area riservata alla replica di tutti i dati dell'ente sia essi file o archivi che backup consolidati dei dati gestiti dagli applicativi software.

L'Ente dispone inoltre di 2 server

Procedura Operativa P.PSDR.02

Tipo VM	Descrizione	Responsabilità
Server Applicativo	Server su cui installare le procedure gestionali e le relative share di rete	AP Systems Cloud avrà il Compito di mantenere e rendere disponibile la VM, vigilare sulla corretta procedura di backup durante il periodo del suo utilizzo. Inoltre dovrà garantire la disponibilità di connettività sul Sito Secondario ed il servizio di VPN. I responsabili tecnici dell'ente hanno il compito di gestire in maniera autonoma e/o con il supporto dei propri tecnici esterni specialistici tutte le operazioni di attivazione del sito, installazione e configurazione del server, nonché il restore dei dati

Nell'Ente sono state individuate 2 postazioni di lavoro operative in caso di emergenza per ogni Servizio erogato appartenente alla CLASSE 1 e 2 descritto nel paragrafo 3.4.

In caso di interruzione dei servizi di connettività sul Sito Primario sarà attivato un collegamento Internet su rete mobile con le opportune garanzie di sicurezza del canale (VPN).

3.2.3 Procedura di ripristino delle banche dati nel sito secondario

La procedura di ripristino delle banche dati tiene in considerazione due diverse situazioni a seconda dell'entità dell'evento e tipologia dei dati:

Procedura Operativa P.PSDR.03

Tipo di banca dati	Descrizione	Responsabilità
File e Archivi	I File / Archivi gestiti dai software di Office Automation vengono ripristinati dal software di replica a partire dalla copie disponibili nelle aree di backup del Sito Secondario. I file sono resi disponibili, con le opportune policy di sicurezza, attraverso il Client Remoto o tramite condivisione SMB.	AP Systems Cloud avrà il Compito di mantenere e rendere disponibile la VM, vigilare sulla corretta procedura di backup durante il periodo del suo utilizzo. Inoltre dovrà garantire la disponibilità di connettività sul Sito Secondario ed il servizio di VPN. I responsabili tecnici dell'ente hanno il compito di gestire in maniera autonoma e/o con il supporto dei propri tecnici esterni specialistici tutte le operazione di ripristino del file e/o archivi e la corretta configurazione delle policy di sicurezza.
Database strutturati di procedure applicative	I backup consolidati delle banche dati sono trasferiti nella VM dei servizi applicativi e ripristinati secondo le specifiche modalità dettate dalle software house, soprattutto con riferimento alle situazioni di BD in formato proprietario o DBMS specifici.	AP Systems Cloud avrà il Compito di mantenere e rendere disponibile la VM, vigilare sulla corretta procedura di backup durante il periodo del suo utilizzo. Inoltre dovrà garantire la disponibilità di connettività sul sito secondario ed il servizio di VPN. I responsabili tecnici dell'ente hanno il compito di gestire in maniera autonoma e/o con il supporto dei propri tecnici esterni specialistici tutte le operazione di ripristino delle banche dati.

3.2.4 Procedura di ripristino delle applicazioni nel sito secondario

Procedura Operativa P.PSDR.04

Il responsabile della Continuità operativa e Responsabile CED dell'Ente, avvalendosi della collaborazione dei tecnici interni o dei tecnici esterni, identifica tutti i software applicativi utili nelle attività ordinarie. L'elenco dei software e procedure di installazione necessarie per garantire i servizi in caso di emergenza sono individuate in base alla gravità ed entità dell'evento disastroso.

3.2.5 Procedura per la gestione dell'organizzazione logistica e coordinamento del personale

La procedura definisce le attività da compiere per fronteggiare una prima fase di emergenza indipendentemente dalla gravità dell'evento disastroso.

Procedura Operativa P.PSDR.05

Tipo di Evento	Evento	Azione	Responsabilità	Ordine di esecuzione e Priorità
Infrastrutture fisiche (edifici)	Distruzione completa o parziale o inagibilità di alcune aree fisiche	Individuazione di un sito alternativo	Comitato di Gestione della Crisi /Resp. Ufficio Tecnico	1 – ALTA
Infrastrutture fisiche (edifici)	Distruzione completa o parziale o inagibilità di alcune aree fisiche	Predisposizione di connessione dati ai sistemi informativi centrali del Sito Primario o di connessione con il sito DR (Sito Secondario)	Comitato di Gestione della Crisi /Resp. Ufficio Tecnico/ Resp. CED	2 - ALTA

Infrastrutture fisiche (edifici)	Distruzione completa o parziale o inagibilità di alcune aree fisiche	Dotazione di postazioni informatiche, adeguate al collegamento con il sito DR, ad un nucleo di personale dell'ente individuato come necessario per fronteggiare la crisi	Comitato di Gestione della Crisi /Resp. CED	3 - ALTA
-------------------------------------	---	---	---	----------

3.3 Ripristino del sito di produzione

3.3.1 Condizioni per il ritorno al sito di produzione

Il piano di ripristino dei sistemi sul sito primario ha l'obiettivo di documentare tutte le procedure previste per ripristinare i sistemi e i ritornare ad una normale operatività.

Generalmente viene predisposto quando tutte le facilities presenti sono state ripristinate e sono in grado di supportare tutte le funzionalità previste in precedenza.

L'attività di rientro al sistema di produzione viene concordata e pianificata dal Comitato di Gestione della crisi.

Una volta che l'infrastruttura risulterà ripristinata e pronta ad accogliere il ritorno dei sistemi, si procederà alla realizzazione dei seguenti passi:

- a) Identificazione del primo periodo utile per la migrazione. Ove possibile si preferirà la pianificazione dell'attività durante un week-end
- b) Comunicazione all'utenza della indisponibilità dei servizi per circa 24h.
- c) Ripristino delle normali policy di accesso ai sistemi dalla rete geografica.

Procedura Operativa P.RSP.01

SOGGETTI AZIONI	Comitato di Gestione della Crisi	CED	TEMPI	Note, Registrazioni, Mod., Istruzioni Operative
Adozione della decisione di ripristino del sito primario				
Verifica della situazione e Coordinamento con il Comitato di Gestione della Crisi				
Check della situazione nel Sito Primario				
Check sullo stato attuale delle risorse, dati, procedure applicative nel sito Secondario e Stima della Mole di Dati da trasferire nel sito Primario				Scelta della modalità di Trasferimento dati dal sito secondario al sito primario
Pianificazione del Week-End per Eseguire il ripristino				Il Responsabile della CO e Responsabile CED Pianifica le attività con i propri collaboratori e con il Comitato di Gestione della Crisi le attività di comunicazione verso la cittadinanza e dipendenti
Esecuzione delle Copie dell'intero Ambiente Secondario per poter essere trasferito nel sito Primario				
Trasferimento dei Dati dal Sito Secondario al Sito Primario				Procedura Operativa P.RSP.02
Procedura di ripristino dell'infrastruttura				Procedura Operativa P.RSP.03
Procedura di ripristino della banche dati				Procedura Operativa P.RSP.04
Procedura di ripristino delle applicazioni				Procedura Operativa P.RSP.05
check Finale del Sito Primario				
Configurazione delle Postazioni Client Presso L'Ente				
Ripresa della Attività Operative dal parte degli operatori dell'ente nel Sito Primario				

3.3.2 Procedura per il trasferimento dei dati dal sito secondario al sito primario

La procedura di trasferimento dati varia a seconda della mole di dati di trasferire fra i due siti.

Procedura Operativa P.RSP.02

Perdita completa del sito primario	Il trasferimento dati dal sito secondario al sito primario avviene tramite cloud		
Perdita parziale del sito primario	A seconda della criticità ed importanza del servizio vengono adottate le seguenti procedure		
	Criticità del Servizio definita paragrafo 10.1	Quantità espressi in GB	Modalità di ripristino
	Classe 1	Superiore a 20 GB	Automatica su cloud
	Classe 1	Inferiore 20 GB	Automatica su cloud
	Classe 2 e Classe 3	Superiore a 50 GB	Automatica su cloud
	Classe 2 e Classe 3	Inferiore 50 GB	Automatica su cloud

3.3.3 Procedura Ripristino dell'infrastruttura nel sito primario

Il ripristino del sito primario prevede la verifica della corretta configurazione degli apparati hardware e software prima di eseguire qualsiasi operazione di ripristino delle banche dati:

Procedura Operativa P.RSP.03

Sicurezza Fisica	- Verifica della continuità elettrica e climatizzazione dei locali adibiti ad ospitare gli apparati di comunicazione; - Verifica del corretto ripristino dell'hardware o collaudo dell'eventuale nuovo hardware acquistato; - Verifica di tutte le postazioni client danneggiate;
Sicurezza Logica	- Verifica di tutte le configurazioni e policy di sicurezza dell'ente;
Connettività e Connessioni dati	- Check della connessione internet e/o SCP; - Verifica della corretta configurazione di tutti gli apparati di rete interni;

3.3.4 Procedura Ripristino della banche dati nel sito primario

Procedura Operativa P.RSP.04

Il ripristino delle banche dati tiene conto della loro tipologia come nel caso dell'attivazione del sito Secondario.

Per i file o archivi gestibili tramite gli strumenti di Office Automation vengono ripristinati nelle share di rete secondo la struttura di competenza e le politiche di sicurezza definite nell'ente.

Il ripristino dei Data base vengono eseguiti dai tecnici specializzati della software house fornitrice del software.

3.3.5 Procedura Ripristino delle applicazioni nel sito primario

Procedura Operativa P.RSP.05

Postazioni Client	- Installazione e/o Check di tutto il software necessario all'operatore - Verifica della corretta configurazione degli apparati esterni (scanner, stampanti ecc.) disponibili nella postazione
-------------------	---

Server Applicativi	- Installazione e/o Check di tutto il software necessario al ripristino funzionale del sistema - Ripristino dei backup - Verifica di collegamento delle postazioni Client - Verifica della corretta configurazione degli apparati esterni (stampanti ecc.); - Verifica delle procedure di backup/aggiornamento
--------------------	--

4 Formazione

La formazione delle risorse riveste un ruolo fondamentale per assicurare la corretta applicazione, conoscenza e padronanza del Piano. Periodicamente è necessario verificare il livello di formazione di tutte le risorse coinvolte nel PCO ICT affinché ciascuna sia ben consapevole delle attività da svolgere in caso di Emergenza. Tutte le risorse coinvolte nel PCO ICT devono essere formate ed istruite circa l'applicazione delle procedure e modalità da seguire nelle diverse attività sia ordinarie sia di emergenza. Il Responsabile della Continuità Operativa ICT assicurare un'efficace pianificazione della formazione sia in termini di periodicità sia di contenuti.

I passi da seguire sono:

- Redazione del piano di formazione
- Redazione del programma di formazione
- Test per la valutazione del livello di conoscenza del Piano
- Relazione di sintesi dei risultati dell'attività formativa

5 Verifica/test del piano

5.1 Obiettivi e strategie di test

Per assicurare una effettiva efficienza nelle operazioni di recovery è prevista l'esecuzione di prove almeno semestrali di funzionalità sia tecnica che organizzativa delle procedure di recovery predisposte. Le prove di recovery coinvolgeranno un sottoinsieme significativo degli utenti del Sistema Informativo, in modo da verificare l'effettiva funzionalità dell'intero processo.

Viene data evidenza dell'esito dei test effettuati in apposite schede, che vengono poi consegnate all'Amministrazione.

5.2 Procedure di test e verifica

La responsabilità dell'esecuzione dei test di continuità operativa è dell'Amministrazione. I tecnici di delle aziende fornitrici forniscono assistenza durante queste fasi, secondo quanto opportunamente concordato con l'amministrazione.

La procedura di test e verifica di un evento disastroso e la valutazione della capacità della soluzione proposta di garantire il livello di continuità operativa atteso, in termini tecnologici, organizzativi e procedurali.

Sono possibili numerose modalità di test, eseguite anche contemporaneamente, nel corso di un anno che comprendono almeno: due verifiche teoriche ed una simulazione.

In funzione di esigenze specifiche di organizzazione e/o di cambiamento potranno essere eseguiti ulteriori test.

Si individuano le seguenti tipologie di procedure di test, elencate in ordine crescente di complessità:

- **Verifica teorica:** E' la metodologia più classica, e ricalca le usuali tecniche di auditing e di validazione "su carta". Consiste nel condurre un'analisi di congruenza della soluzione, a cura degli stessi autori della soluzione o di esperti esterni.
- **Verifica strutturata:** Si definisce uno specifico scenario teorico di crisi, e i partecipanti al test operano pedissequamente secondo le modalità previste dal Piano di Continuità operativa. Nel corso della sequenza si verificano e documentano eventuali errori o carenze.
- **Simulazione.** In questo caso il test coinvolge l'intero personale dell'amministrazione o almeno il personale addetto all'area interessata dalla simulazione. Il test prevede l'attivazione "in tempo reale" del piano di continuità operativa e la verifica delle procedure, dei sistemi di backup, dei sistemi alternativi di comunicazione, della mobilitazione dei gruppi di gestione dell'emergenza, del recupero di documenti e dati. Condurre una simulazione di emergenza completa può avere un costo molto elevato; per questo in genere si usano simulazioni semplificate.

Quando sono previsti test periodici di simulazione, valgono i seguenti requisiti:

- le simulazioni devono essere progettate per simulare una "vera" condizione di emergenza, ricreando le conseguenze dell'evento peggiore nel peggior momento tra quelli valutati negli scenari di Risk Assessment (ad esempio, l'improvvisa indisponibilità del Sito Primario durante l'orario di punta dei servizi erogati);
- per non rischiare di compromettere i dati di produzione, per lo svolgimento delle simulazioni, dovranno essere predisposte copie coerenti dei dati ad uso esclusivo della simulazione che saranno cancellate al termine delle prove;
- poiché la soluzione prevede un centro alternativo (nodo secondario del sito secondario), è necessario verificare e testare tutti quei processi e procedure che devono garantire, in condizioni di funzionamento normale del centro primario, le operazioni di allineamento dei due siti.

6 Manutenzione del piano

6.1 Aggiornamento del piano

Il presente piano viene aggiornato entro il 31 dicembre dal RTD come indicato all'articolo 50 bis del D.lgs 82/2005, il processo e le regole di redazione sono riportate nel seguito:

Le modifiche apportate ad uno qualsiasi dei documenti che costituiscono il Piano, siano essi manuali o allegati esterni, ne comporterà una variazione di modifica e/o release.

Al fine di determinare univocamente la versione/release del Piano, si adotta la seguente metodologia di numerazione:

MAJOR RELEASE . MINOR RELEASE

La modifica di un manuale o di un allegato esterno che scaturisca da una manutenzione ordinaria darà luogo a una nuova minor release del documento (passerà da m.n a m.n+1 ad esempio si passerà dalla release 1.0 alla release 1.1). La modifica di un manuale o di un allegato esterno che scaturisca da una manutenzione straordinaria darà luogo a una nuova major release del documento (passerà da m.n a m+1.0 ad esempio si passerà dalla release 1.5 alla release 2.0).

Dovranno essere aggiornati di conseguenza i dati di controllo presenti nella copertina del documento, la versione nel piè di pagina e la data nell'intestazione.

A ogni nuova versione o release di uno dei documenti che costituiscono il Piano sarà creata una nuova versione o release dell'allegato esterno, tale modifica andrà riportata nella tabella contenuta nel paragrafo 1 "Informazioni Generali" contenente gli estremi delle ultime versioni o release modificate.

La copia cartacea delle nuove versioni o release dovrà essere firmata per approvazione sulla copertina dal responsabile del Gruppo di supporto unitamente alla data di approvazione. Dopo la firma, dovrà essere aggiornata la copia magnetica inserendo il nome del responsabile del Gruppo di supporto e la data di approvazione, e archiviato il documento in formato magnetico/cartaceo secondo lo standard definito.

A ogni nuova versione/release dei documenti che costituiscono il Piano, il Comitato di Gestione della Crisi ha il compito di curare la distribuzione dello stesso affinché le "copie ufficiali" del Piano siano sempre aggiornate.