Comune di Parma

PIANO DI BUSINESS CONTINUITY

Documento per approvazione formale ai fini ID.IM-04

Comune di Parma

Questo documento è confidenziale. Le informazioni confidenziali non devono essere divulgate a terze parti diverse dai dipendenti e dai fornitori autorizzati da Comune di Parma e IT.CITY con apposita autorizzazione scritta. Le terze parti autorizzate potranno solo prendere visione della versione cartacea o digitale del documento presso le sedi del Comune di Parma e di IT.CITY. Le informazioni confidenziali devono essere tenute in luogo sicuro e non devono essere riprodotte o usate per scopi non autorizzati da Comune di Parma e IT.CITY. La riproduzione può avvenire solo con l'autorizzazione del Comune di Parma e di IT.CITY e le copie devono recare la classificazione dei documenti originali.
I documenti originali sono conservati e consultabili nel repository documentale sharepoint Settore Transizione Digitale - Pagina iniziale).

Redazione, Variazioni, Approvazioni

Redazione

Autore:
Data di creazione: 15/01/2026
Ultimo aggiornamento:
Codice:
Versione: 1.1
Stato:
Classificazione: INTERNO

Variazioni

Data	Autore	Versione	Variazione
03/06/2026	Settore Sviluppo Economico e Transizione Digitale	1.1	Adeguamento ISO/IEC 27001:2022 e NIS2 (D.Lgs. 138/2024)

Approvazioni

Nome	Funzione	Data	Firma
Nicola Ferioli	Dirigente del Settore Sviluppo Economico e Transizione Digitale	29/06/2026	

Lista distribuzione

L'elenco delle risorse che accedono al documento è gestito e visibile sulla cartella che lo contiene su SharePoint on-line/Intranet

IT.CITY S.P.A. (Società in house, controllata – a socio unico – sottoposta all'attività di direzione e coordinamento del Comune di Parma) tramite contratto stipulato in data 23 maggio 2022 Rep. N. 19608 della Raccolta Scritture Private del Comune di Parma, maggio 2022 - aprile 2025, e rinnovato fino ad aprile 2028 mediante la stipula del contratto Rep. SP/20365/2025 del 4 luglio 2025, è stata nominata Gestore del Sistema Informatico Comunale di Parma. Il presente documento, ai sensi del Contratto sopracitato, garantisce lo sviluppo coerente e l'integrazione di nuove tecnologie nell'intero sistema informativo dell'Ente e definisce le procedure e le istruzioni sicurezza per una gestione efficace e completa.

Comune di Parma

SOMMARIO

ACRONIMI E DEFINIZIONI 5
RIFERIMENTI NORMATIVI E DOCUMENTALI 6
1 INTRODUZIONE 7
1.1 SCOPO E OBIETTIVO DEL DOCUMENTO 7
1.2 CAMPO DI APPLICAZIONE 7
2 CONTESTO E ANALISI PRELIMINARI 7
2.1 ANALISI DEI RISCHI E DEGLI SCENARI DI INTERRUZIONE 7
2.2 IMPATTI SULL'AMMINISTRAZIONE (COLLEGAMENTO CON LA BIA) 8
2.3 MAPPA DELLE RISORSE E INFRASTRUTTURE CRITICHE 8
2.3.1 RISORSE INFRASTRUTTURALI 9
2.3.2 RISORSE APPLICATIVE E SISTEMI INFORMATIVI CRITICI 9
2.3.3 RISORSE ORGANIZZATIVE E FORNITORI DI SUPPORTO 9
3 GESTIONE DELLA BUSINESS CONTINUITY 10
3.1 GOVERNANCE, RUOLI E RESPONSABILITA' 10
3.2 PROCESSO DI GESTIONE DELLA CONTINUITA' OPERATIVA 11
3.2.1 RILEVAZIONE 11
3.2.2 ATTIVAZIONE 11
3.2.3 NOTIFICA 12
3.2.4 GESTIONE DELL'EMERGENZA 12
3.2.5 GESTIONE DEL DISASTRO E DELLA CRISI 13
3.2.6 RIPRISTINO E RIENTRO ALLA NORMALITÀ 13
3.3 SOLUZIONI E STRATEGIE DI CONTINUITA' OPERATIVA 14
3.3.1 INDISPONIBILITÀ DEI SISTEMI ICT 14
3.3.2 INDISPONIBILITÀ DELLE SEDI OPERATIVE 14
3.3.3 INDISPONIBILITÀ DEL PERSONALE 14
3.3.4 INDISPONIBILITÀ DEI FORNITORI 15
4 MODALITA' DI COMUNICAZIONE 15
4.1 FLUSSI E CANALI DI COMUNICAZIONE 15
4.2 COMUNICAZIONI INTERNE 15
4.3 COMUNICAZIONI ESTERNE 16
5 FORMAZIONE 16
6 MANTENIMENTO E REVISIONE DEL PIANO 16
6.1 PERIODICITA' E CRITERI DI AGGIORNAMENTO 16
6.2 REGISTRO DELLE VERSIONI E RESPONSABILITA' DI REVISIONE 17
6.3 INTEGRAZIONE CON ALTRI PIANI 17
ALLEGATI 18
SCHEDE DI BUSINESS IMPACT ANALYSIS 18
PIANO DI DISASTER RECOVERY 18
ELENCO CONTATTI DI EMERGENZA 18
TEMPLATE DI COMUNICAZIONI 18

ACRONIMI E DEFINIZIONI

Definizione/acronimo	Descrizione
Business Continuity	Capacità dell'organizzazione di proseguire nell'erogazione di servizi/produzione di beni con predefiniti livelli prestazionali a seguito di incidenti/disastri che possano causarne l'interruzione.
BCP	Business Continuity Plan.
Compliance	Conformità a leggi, regolamenti, standard e politiche aziendali.
BIA	Business Impact Analysis.
GDPR	*General Data Protection Regulation – reg. UE 2016/679* - Regolamento (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.
RPO	Punto di ripristino (Recovery Point Objective): indica l'istante di consolidamento dei dati fino al quale è garantita l'integrità degli stessi.
RTO	Tempo di ripristino (Recovery Time Objective): rappresenta il massimo tempo di indisponibilità di un servizio o, in altri termini, la velocità con la quale è necessario ripristinare il servizio fermo.
Resilienza operativa	Capacità di un sistema o processo di continuare a funzionare in caso di eventi avversi o imprevisti.
Crisi	Situazione eccezionale, per sua natura di bassa probabilità, il cui verificarsi comporta per l'organizzazione perdite economiche, materiali, umane o ambientali tali da superare la capacità dell'organizzazione stessa di rispondere e ripristinare l'operatività prima che tali perdite causino un impatto critico per il business.
Evento di indisponibilità	Situazione con impatto significativo in un'area circoscritta o non circoscritta, che abbia generato o che possa generare danni rilevanti, quali ad esempio la perdita di risorse umane, edifici o asset, sistemi informativi o infrastrutture di rete, informazioni critiche.
Impatto	Misura di gravità di un evento avverso che determina un danno ai processi o agli asset aziendali.
Incidente	Evento che può generare un'interruzione, una perdita, un'emergenza o una crisi in relazione alle attività aziendali.
Minaccia	Evento interno o esterno all'azienda che può determinare l'interruzione del processo Gestione Esercizio Metropolitane in relazione all'esistenza di vulnerabilità.
Rischio	Combinazione tra la probabilità di accadimento di un incidente o evento di crisi e l'impatto sul business che tale incidente/evento potrebbe causare.
Processo di Business Continuity	Processo di gestione complessiva volto a identificare le minacce ai processi di business, valutarne l'impatto e aumentare la resilienza dei processi aziendali attraverso la definizione di un'adeguata strategia di risposta, assicurando la Continuità Operativa.

Comune di Parma

RIFERIMENTI NORMATIVI E DOCUMENTALI

Il Business Continuity Plan è redatto in conformità con le principali normative e standard in materia di continuità operativa e sicurezza delle informazioni, tra cui:

- **ISO 22301:2019** - *Security and resilience - Business continuity management systems - Requirements*, standard internazionale di riferimento per i sistemi di gestione della continuità operativa.
- **ISO 22313:2020** - Linee guida per l'implementazione del sistema di gestione della continuità operativa.
- **ISO/IEC 27001:2022** - Standard per la gestione della sicurezza delle informazioni, con controlli rilevanti per la continuità operativa.
- **ISO/IEC 27031:2011** - Linee guida per la preparazione delle ICT alla continuità operativa.
- **ISO 31000:2018** - Linee guida per la gestione del rischio, utile per l'analisi dei rischi nel BCP.
- **Regolamento (UE) 2016/679 (GDPR)** - Obblighi per la protezione dei dati personali, inclusa la continuità dei servizi che li trattano.
- **D.Lgs. 231/2001** - Rilevanza dei modelli organizzativi e dei presidi di controllo (continuità inclusa) per la responsabilità amministrativa dell'ente.
- **Direttiva NIS2 (UE) 2022/2555** - Requisiti di sicurezza informatica e continuità dei servizi essenziali per operatori dei settori critici.
- **D.Lgs. 4 settembre 2024, n. 138**, in particolare artt. 23, 24 e 25, per governance, continuità operativa, backup, disaster recovery, gestione delle crisi e notifica degli incidenti significativi.
- **Determinazione ACN n. 164179** del 14 aprile 2025 e Allegato 1 "Misure di sicurezza di base per i soggetti importanti", con particolare riferimento alla misura ID.IM-04.
- **ISO/IEC 27002:2022**, controllo A.5.30 "ICT readiness for business continuity", e controllo A.5.23 per la sicurezza delle informazioni nell'uso dei servizi cloud.
- **Contratti di servizio e SLA con fornitori critici**, considerati come riferimenti vincolanti per la continuità dei servizi esternalizzati.
- Framework documentale specifico Comune di ParmaFramework documentale IT.CITY S.P.A. Sistema di Gestione della Sicurezza delle Informazioni (SGSI)
-

1 INTRODUZIONE

1.1 SCOPO E OBIETTIVO DEL DOCUMENTO

Il Comune di Parma adotta un proprio modello organizzativo e di governo per la gestione della sicurezza delle informazioni e della cybersicurezza, nell'ambito del quale sono definiti ruoli, responsabilità, autorità e funzioni di indirizzo, governo, supervisione e controllo.
Per l'attuazione operativa di tale modello, il Comune si avvale del Sistema di Gestione per la Sicurezza delle Informazioni (SGSI) adottato da IT.CITY S.p.A., società in house dell'Ente, nonché delle relative politiche, procedure, metodologie e misure di sicurezza, per quanto applicabili ai servizi affidati e al perimetro comunale.
Restano in capo al Comune di Parma la governance complessiva della sicurezza, l'indirizzo strategico, il governo e l'accettazione del rischio, l'approvazione delle misure e dei piani di propria competenza, la supervisione e la vigilanza sulla loro attuazione, in conformità al Decreto Legislativo 4 settembre 2024, n. 138 e alle altre disposizioni applicabili in materia di cybersicurezza.

Il presente Piano disciplina il modello adottato dal Comune di Parma per la gestione delle vulnerabilità nell'ambito del proprio sistema di governo della sicurezza delle informazioni. Per le attività operative relative ai sistemi e servizi affidati, il Comune si avvale di IT.CITY S.p.A., che opera secondo il proprio SGSI e, in particolare, secondo la Politica POL-SGSI-017 "Piano di Business Continuity",. Restano in capo al Comune le funzioni di indirizzo, approvazione, supervisione, vigilanza e governo del rischio.
Il presente Piano di Business Continuity (di seguito, anche: "BCP") definisce il modello organizzativo, le procedure e le azioni necessarie a garantire la continuità dei servizi essenziali del Comune di Parma in caso di eventi che compromettano la normale operatività.

L'obiettivo principale è assicurare che l'Amministrazione sia in grado di:
- reagire tempestivamente a interruzioni operative o emergenze di diversa natura;
- ridurre al minimo l'impatto sull'erogazione dei servizi, sui cittadini e sui fornitori;
- ripristinare le attività critiche entro tempi compatibili con le esigenze dell'amministrazione e con le disposizioni normative vigenti.

Il piano costituisce uno strumento operativo e di coordinamento, utile sia in fase di emergenza sia nella pianificazione preventiva delle misure di resilienza. Esso si integra con gli altri strumenti di gestione del rischio e della sicurezza in uso presso il Comune, tra cui il Piano di Disaster Recovery (DRP). Il BCP rappresenta il quadro generale delle strategie e delle misure organizzative adottate per garantire la continuità operativa del Comune, mentre il DRP costituisce una componente tecnica del presente Piano, focalizzata sulle procedure di ripristino delle infrastrutture e dei sistemi ICT a supporto dei processi critici.

1.2 CAMPO DI APPLICAZIONE

Il BCP si applica all'intera organizzazione del Comune di Parma e ha l'obiettivo di assicurare la continuità operativa dei servizi essenziali in caso di eventi che comportino un'interruzione, parziale o totale, delle normali attività dell'Amministrazione. Il piano rappresenta uno strumento di gestione e coordinamento delle azioni necessarie a garantire la ripresa dei servizi critici entro i tempi massimi accettabili, riducendo gli impatti sull'operatività, sui cittadini e sull'immagine istituzionale del Comune. Il piano definisce le regole generali di gestione della continuità

operativa e si applica a tutti i servizi e processi critici che concorrono alla funzionalità dell'Amministrazione.
Il Piano è redatto, attuato, verificato e migliorato nel quadro del SGSI. Gli scenari, le priorità e le strategie di continuità derivano dalla Business Impact Analysis e dal processo PR-SGSI-001; i controlli applicabili sono tracciati nella Dichiarazione di Applicabilità. Gli esiti di test, incidenti e attivazioni alimentano il Registro dei Rischi e il Piano di Trattamento/Adeguamento, assicurando coerenza con le clausole 4-10 della ISO/IEC 27001:2022.
Il BCP si applica a tutti gli eventi, intenzionali o accidentali, che possano determinare l'interruzione totale o parziale delle attività del Comune di Parma, tra cui:

- indisponibilità delle infrastrutture ICT (server, rete, sistemi applicativi);
- attacchi informatici o incidenti di sicurezza (ransomware, malware, data breach, blocchi di servizi digitali);
- eventi fisici o ambientali (incendi, allagamenti, blackout prolungati, guasti strutturali alle sedi);
- indisponibilità del personale chiave o impossibilità di accesso alle sedi operative;
- interruzioni dei servizi erogati da fornitori o partner tecnologici (inclusi i servizi gestiti da IT.CITY).

2 CONTESTO E ANALISI PRELIMINARI

2.1 ANALISI DEI RISCHI E DEGLI SCENARI DI INTERRUZIONE

L'analisi dei rischi rappresenta la fase preliminare e fondamentale per la definizione delle misure di continuità operativa. Essa consente di individuare le minacce potenziali e gli scenari di interruzione che potrebbero compromettere la regolare erogazione dei servizi comunali.
Le principali categorie di rischio che possono incidere sulla disponibilità dei servizi e dei sistemi ICT sono:

- Rischi tecnologici e infrastrutturali: guasti hardware o software, malfunzionamenti di rete, corruzione di dati, indisponibilità dei server applicativi o dei database che supportano i sistemi gestionali (es. applicativi di protocollo e anagrafe).
- Rischi informatici e di sicurezza: attacchi ransomware, malware, phishing, data breach o compromissioni dei sistemi di autenticazione e accesso.
- Rischi fisici e ambientali: incendi, allagamenti, blackout elettrici, guasti agli impianti di climatizzazione o di alimentazione dei data center, eventi meteo estremi.
- Rischi organizzativi e operativi: errori umani, carenze di competenze, processi non documentati o dipendenza da figure chiave.
- Rischi derivanti da terze parti: indisponibilità dei fornitori ICT, interruzione di servizi cloud o di connettività, ritardi negli interventi di assistenza tecnica.

Ciascuno di questi scenari può avere un impatto differente sui processi gestiti dall'Amministrazione.

2.2 IMPATTI SULL'AMMINISTRAZIONE (COLLEGAMENTO CON LA BIA)

La Business Impact Analysis (BIA) condotta dal Comune di Parma ha consentito di individuare i processi prioritari ai fini della continuità operativa, nonché di stimare gli impatti economici, reputazionali e operativi derivanti da un'interruzione.

Dall'analisi sono emersi come processi critici:

- il Servizio Protocollo;
- i Servizi Demografici.

Gli impatti principali rilevati sono:

- Impatto operativo: blocco o ritardo nell'erogazione dei servizi al cittadino e nei flussi documentali interni.
- Impatto normativo e legale: mancato rispetto degli obblighi di legge e delle scadenze amministrative (es. protocollazione, certificazioni anagrafiche, atti ufficiali).
- Impatto reputazionale: perdita di fiducia da parte dei cittadini e percezione di inefficienza istituzionale.
- Impatto economico: costi aggiuntivi per interventi tecnici straordinari, recupero dati o servizi sostitutivi.

Per ciascun processo analizzato sono stati definiti i tempi massimi di ripristino (RTO) e i periodi massimi di ripristino (RPO) che costituiscono parametri di riferimento per le strategie di continuità operative descritte nei capitoli successivi.
Per ogni processo e servizio critico la BIA deve documentare e mantenere approvati almeno: impatto nel tempo, tempo massimo tollerabile di interruzione, livello minimo accettabile di servizio, RTO, RPO, dipendenze tecnologiche e organizzative, risorse minime e priorità di ripristino. I valori devono essere validati dai responsabili di processo e riesaminati a seguito di variazioni rilevanti, incidenti, test o modifiche dei fornitori.

2.3 MAPPA DELLE RISORSE E INFRASTRUTTURE CRITICHE

La continuità dei servizi essenziali del Comune di Parma si fonda su un insieme di risorse infrastrutturali, applicative e organizzative la cui disponibilità è determinante per l'erogazione delle funzioni istituzionali e dei servizi digitali ai cittadini. La presente sezione fornisce una mappatura sintetica delle principali risorse critiche, in coerenza con quanto emerso dalla Business Impact Analysis e in raccordo con il Piano di Disaster Recovery.

2.3.1 Risorse infrastrutturali

Le infrastrutture ICT rappresentano la base tecnica su cui si appoggiano i sistemi e i servizi dell'Ente.
Esse comprendono:

- i data center e i siti tecnologici gestiti da IT.CITY S.p.A. e da Lepida S.c.p.A., presso i quali risiedono le principali piattaforme applicative e le componenti di virtualizzazione e storage;
- la rete cittadina MPLS che garantisce la comunicazione tra tutte le sedi operative del Comune;
- la rete dati interna che garantisce la comunicazione delle postazioni di lavoro verso i servizi interni (Data Center) o cloud (SaaS);
- le infrastrutture di sicurezza e connettività (firewall, VPN, apparati di rete) che assicurano l'accesso sicuro ai sistemi;
- i sistemi di continuità elettrica (UPS) e le forniture energetiche ridondate, necessari al mantenimento dell'operatività dei data center;
- le postazioni di lavoro, i dispositivi mobili e i terminali utilizzati dal personale per l'erogazione dei servizi quotidiani.

Le misure di disponibilità, replica e ripristino di tali componenti sono descritte in dettaglio nel Piano di Disaster Recovery, che ne disciplina gli aspetti tecnici.
Per le infrastrutture Cloud e i servizi SaaS utilizzati, la continuità operativa, il ripristino dei servizi e la gestione degli incidenti sono in capo ai fornitori, secondo i livelli di servizio (SLA)

contrattualmente definiti. L'Amministrazione porta avanti attività di monitoraggio e coordinamento, demandando al fornitore la risoluzione di eventuali disservizi.
L'esternalizzazione a fornitori cloud o SaaS non trasferisce la responsabilità del Comune. Per i servizi rilevanti devono essere definiti e verificati: modello di responsabilità condivisa, requisiti di disponibilità e resilienza, RTO/RPO contrattuali, backup ed esportabilità dei dati, portabilità e strategia di uscita, continuità dei subfornitori, obblighi di notifica a cascata, canali di emergenza ed evidenze dei test di ripristino. Le eventuali carenze sono registrate come rischio e trattate tramite il Piano di Adeguamento.

2.3.2 Risorse applicative e sistemi informativi critici

I servizi core e quelli individuati come critici nella BIA, si basano su un insieme di applicativi e piattaforme informatiche la cui disponibilità è essenziale per l'operatività dell'Amministrazione.
Tra i principali:

- sistemi gestionali per la demografia e lo stato civile;
- sistemi di protocollo informatico e gestione documentale;
- portali e servizi digitali rivolti ai cittadini;
- piattaforme di posta elettronica istituzionale e PEC;
- sistemi Polizia Locale (es. videosorveglianza, controllo targhe, centrale operativa);
- sistema istruttoria atti monocratici e collegiali (Iter-Atti);
- sistema gestionale settore Educativo;
- sistema gestionale settore Sociale;
- sistema gestionale settore Risorse Umane.

2.3.3 Risorse organizzative e fornitori di supporto

Oltre alle componenti tecnologiche, la continuità operativa dipende da risorse organizzative e da fornitori esterni che garantiscono il funzionamento complessivo dei servizi.
Tra cui:

Fornitore	Servizio erogato
Ads Automated Data Systems S.p.A.	Suite GIPSI - Gestione Personale, Sfera e Albo Online - Iter atti, Casa di Vetro (L190) - Trasparenza
Anthesi S.r.l.	Piattaforma Elixform per configurazione ed erogazione di Servizi online
Bridge 129 Safety & Security S.r.l.	Videosorveglianza
Cts S.r.l.	Videosorveglianza - TSCAN monitoraggio traffico
Dromedian S.r.l.	Sistema conferenza e votazione Consiglio Comunale
Ecoh Media S.r.l.	Strategic PA - gestione società partecipate
Euforlegal S.r.l.	Teleforum FOR - Avvocatura
Gemmlab S.r.l.	Gemello digitale
Gruppo Marche Informatica S.r.l.	SW Cimiteri, SW Contratti
I.T. Ing. Trasp S.r.l.	Sfinge - gestione incidenti
Incloud Team S.r.l.	Connet - Processo sanzionatorio in strada
Lepida S.C.P.A.	Data center, Piattaforma ASTREA per depositi giudiziari
Maggioli S.p.A.	Suite Sicr@Web per Demografici, Stato Civile e Ragioneria, Icaro per Gestione Sociali, CatView - Catasto
Municipia S.p.A.	Engramma – protocollo e gestione pec
Mondo Edp S.r.l.	IRIS - Timbrature e presenze
Proveco S.r.l.	MC3 - Albo Pretorio

Parma Valore Comune	Gestione Riscossione
Redturtle S.r.l.	Portale Istituzionale e Intranet
Retelit Digital Services S.p.A.	Connettività e fonia
Semenda S.r.l.	Infrastruttura GIS e sistemi cartografici, Toponomastica - gestione stradario e civici
Sistemi E Soluzioni S.r.l.	Sep@Com - Gestione Patrimonio, Bando ERP
Starch S.r.l.	Archiweb - Gestionale edilizia e urbanisitca, CPortlal - Servizi online SUE
Telecom	Connettività e fonia (fissa/mobile)

3 GESTIONE DELLA BUSINESS CONTINUITY

3.1 GOVERNANCE, RUOLI E RESPONSABILITA'

La gestione della continuità operativa del Comune di Parma si fonda su una struttura di governance che definisce ruoli, responsabilità e flussi di comunicazione tra le diverse funzioni coinvolte.

Tale modello garantisce il coordinamento tempestivo delle attività in caso di crisi e la chiarezza decisionale nella fase di ripristino dei servizi critici.

Gli Organi di Amministrazione e Direttivi approvano le modalità di implementazione del presente Piano, ne sovrintendono l'attuazione e ricevono report periodici su test, scostamenti da RTO/RPO, rischi residui e azioni correttive. Il Responsabile per la Transizione Digitale assicura il coordinamento con il SGSI e con IT.CITY; il Business Continuity Manager mantiene il Piano e coordina l'attivazione. Compiti, deleghe, sostituzioni e interfacce con fornitori devono essere formalizzati in una matrice RACI, fermo restando che l'affidamento operativo non trasferisce la responsabilità di governo dell'Ente.

Ruoli principali

- **Vertice dell'Ente (Sindaco)**
  Fornisce l'indirizzo istituzionale, assume le decisioni strategiche in emergenza e autorizza le comunicazioni esterne che hanno impatto su cittadini, imprese e altri stakeholder.
  Owner: Comune di Parma
- **Direttore Generale**
  Coordina l'attuazione del Business Continuity Plan, garantisce il raccordo tra le strutture organizzative, supervisiona i flussi di comunicazione interna ed esterna e assicura la coerenza delle azioni intraprese.
  Owner:
- **Business Continuity Manager**
  Valuta l'evento critico, attiva il Business Continuity Plan, coordina operativamente la gestione dell'emergenza, cura l'emissione degli aggiornamenti informativi e monitora lo stato dei servizi essenziali.
  Owner:
- **Responsabili di Servizio**
  Attuano le misure di continuità nelle rispettive aree, organizzano le attività operative, informano il personale, raccolgono segnalazioni e comunicano le criticità al livello di coordinamento.
  Owner:
- **Responsabile degli aspetti fisici delle sedi**
  Attua misure di continuità nelle rispettive sedi (utility e sistemi ITC)
  Owner:
- **Ufficio di comunicazione**

Owner: Comune di Parma

3.2 PROCESSO DI GESTIONE DELLA CONTINUITA' OPERATIVA

Il processo di gestione della Business Continuity si articola in quattro fasi principali, che descrivono il ciclo completo di risposta e recupero da un evento di crisi. Ogni fase definisce responsabilità, obiettivi e attività da attuare.

3.2.1 Rilevazione

Obiettivo: assicurare una rilevazione tempestiva dell'evento e l'attivazione delle funzioni competenti.

Attività principali:

- rilevazione dell'evento, dell'anomalia o dell'interruzione di un servizio critico da parte delle unità operative, dei sistemi di monitoraggio o dei fornitori;
- comunicazione immediata al BCM da parte del referente o dell'unità operativa coinvolta.

Output: notifica formale dell'attivazione del piano e costituzione del team di crisi.

3.2.2 Attivazione

Obiettivo: garantire l'avvio tempestivo del Piano di Business Continuity in risposta a eventi che impattino i servizi critici.

Attività principali:

- analisi preliminare dell'evento e valutazione della gravità, dell'impatto e della potenziale evoluzione;
- decisione sull'attivazione del Piano di Business Continuity da parte del BCM, secondo le soglie e i criteri definiti;
- avvio delle azioni iniziali previste dal Piano e coordinamento delle prime misure di risposta.

Output: decisione formale di attivazione del Piano di Business Continuity e avvio delle azioni di gestione dell'emergenza.

Di seguito si riporta la tabella contenente i valori di RTO e RPO definiti per ciascun processo a seguito della Business Impact Analysis.
Il parametro di riferimento è l'**RTO**: al superamento delle tempistiche indicate, si rende obbligatoria l'attivazione del presente piano.

Processo	Sottoprocesso	RTO (ore)	RPO (ore)
Demografici	Sicra	2	<4
	Portali	4	<0
	Protocollo	8	<8
	Agenda prenotazioni	24	<24
	Sistema ospedali	8	<8
Protocollo		4	<0
Personale	Stipendi	4	<4
	Provv. Disciplinari	48	<4
	Concorsi	48	<4
	Presenze	96	<4
	Previdenza	168	<4
Educativi	Servizi al Cittadino	12	<4
	Graduatorie / Mense	12	<4

	Diete	12	<4
	Cedole Scolastiche	12	<4
	Servizi Integrativi	168	<4

3.2.3 Notifica

Obiettivo: assicurare una comunicazione tempestiva, strutturata e tracciabile dell'attivazione del Piano.

Attività principali:

- notifica formale dell'attivazione del Piano alle direzioni aziendali interessate;
- comunicazione ai fornitori critici e ai partner esterni coinvolti nella continuità operativa;
- diffusione delle informazioni essenziali sull'evento (natura, servizi impattati, azioni iniziali);
- registrazione e tracciamento delle comunicazioni effettuate secondo le modalità previste.

Output: costituzione operativa del team di crisi e piena consapevolezza degli stakeholder interni ed esterni sull'attivazione del Piano.

La notifica interna di attivazione del BCP non sostituisce gli obblighi di notifica degli incidenti. Quando l'evento può costituire un incidente significativo, il BCM e il RTD attivano senza ritardo la Procedura di Gestione degli Incidenti, affinché siano rispettate la pre-notifica entro 24 ore, la notifica/aggiornamento entro 72 ore e la relazione finale entro un mese mediante i canali ACN/CSIRT Italia. Devono essere preservate le evidenze, la cronologia decisionale e le informazioni necessarie alle Autorità; per gli eventi con dati personali è coinvolto il DPO secondo la normativa applicabile.

3.2.4 Gestione dell'emergenza

Obiettivo: contenere gli effetti immediati dell'interruzione e garantire la sicurezza di persone, dati e infrastrutture.

Attività principali:

- messa in sicurezza delle aree e delle risorse coinvolte;
- isolamento dell'evento (es. blocco rete o sistemi compromessi) in coordinamento con IT.CITY;
- comunicazione tempestiva al personale e alle strutture operative tramite canali ufficiali;
- valutazione dell'impatto sui servizi critici;
- aggiornamento costante del Comitato di Crisi sull'evoluzione dell'emergenza.

Output: contenimento dell'evento e identificazione delle misure immediate di mitigazione.

Di seguito si riporta il dettaglio di gestione operativa in caso di interruzione per ciascun processo.

Processi	RTO	RPO	Flusso gestione emergenza
Demografici			• attivazione di modalità operative alternative per la registrazione dei documenti; • priorità alla protocollazione dei documenti urgenti e obbligatori (es. atti con termini perentori, comunicazioni istituzionali); • sospensione o posticipazione delle attività di protocollazione non critiche; • registrazione temporanea dei flussi documentali, con successiva regolarizzazione; • coordinamento continuo con la funzione ICT per il ripristino dei sistemi informativi.

Protocollo			• attivazione di modalità operative alternative per l'erogazione dei servizi anagrafici essenziali; • priorità all'erogazione dei servizi inderogabili; • sospensione o posticipazione delle attività non critiche; • coordinamento continuo con la funzione ICT per il ripristino dei sistemi informativi.
Personale	4		• attivazione di modalità operative alternative; • coordinamento continuo con la funzione ICT per il ripristino dei sistemi informativi.
Educativi	12	<4	• attivazione di modalità operative alternative; • priorità all'erogazione dei servizi inderogabili; • sospensione o posticipazione delle attività non critiche; • coordinamento continuo con la funzione ICT per il ripristino dei sistemi informativi.

In caso di indisponibilità dei canali ordinari di ricezione o invio (es. PEC), il servizio di protocollo assicura la presa in carico dei documenti attraverso i canali disponibili, garantendo la conservazione dell'evidenza documentale e la successiva corretta registrazione a sistema una volta ripristinate le condizioni ordinarie.
In caso di indisponibilità dei collegamenti con sistemi esterni, il servizio Demografici viene gestito secondo le modalità previste dal contratto, limitando l'erogazione alle attività strettamente necessarie.

3.2.5 Gestione del disastro e della crisi

Obiettivo: garantire la continuità minima dei servizi essenziali e attuare le strategie di ripristino previste dal Piano.

Attività principali:

- attivazione delle procedure di continuità definite nel presente Piano;
- coordinamento delle attività di ripristino dei sistemi informativi e delle comunicazioni essenziali;
- gestione del personale operativo;
- comunicazione verso gli stakeholder interni ed esterni (cittadini, enti partner, fornitori strategici);
- monitoraggio dello stato dei servizi e aggiornamento periodico del Comitato di Crisi;
- registrazione delle azioni intraprese e delle decisioni assunte ai fini di audit e rendicontazione.

Output: mantenimento della funzionalità minima dei servizi critici e progressivo recupero della capacità operativa.

3.2.6 Ripristino e rientro alla normalità

Obiettivo: riportare i servizi e le infrastrutture alle normali condizioni operative, garantendo la chiusura controllata dell'emergenza.

Attività principali:

- completamento delle operazioni di ripristino dei sistemi e delle infrastrutture;
- verifica dell'integrità dei dati e del corretto funzionamento dei servizi;
- comunicazione al personale della ripresa delle attività ordinarie;
- disattivazione progressiva delle misure temporanee adottate durante l'emergenza;

- redazione di un rapporto di chiusura dell'evento (*lesson learned*, azioni di miglioramento, aggiornamento del BCP);
- aggiornamento dei registri e dei documenti correlati (BIA, DRP, policy operative).

Output: ritorno alla piena operatività e validazione formale della chiusura della crisi.

3.3 SOLUZIONI E STRATEGIE DI CONTINUITA' OPERATIVA

Le strategie di continuità definiscono l'insieme delle soluzioni organizzative, tecnologiche e logistiche necessarie a garantire la prosecuzione o il rapido ripristino delle attività critiche in caso di interruzione.

3.3.1 Indisponibilità dei sistemi ICT

In caso di indisponibilità dei sistemi informativi:

- attivazione del Piano di Disaster Recovery per il ripristino dei sistemi e dei dati;
- utilizzo di infrastrutture ridondate o ambienti cloud per la continuità dei servizi essenziali;
- predisposizione di procedure manuali o alternative per garantire la gestione operativa minima;
- aggiornamento costante dei referenti di processo sull'avanzamento delle attività di ripristino.

La prontezza ICT per la continuità operativa, in attuazione del controllo A.5.30, comprende ridondanza e capacità adeguata, backup protetti e prove di ripristino, configurazioni documentate, disponibilità di procedure e contatti offline, canali di comunicazione di emergenza protetti, registrazione degli eventi, sincronizzazione temporale, controllo degli accessi privilegiati e modalità operative manuali. Il ripristino deve avvenire da copie verificate e in ambienti considerati affidabili, senza ridurre i requisiti minimi di sicurezza durante l'emergenza.

In caso di indisponibilità dei sistemi informativi in SaaS:

- coordinamento con i fornitori per stabilire i tempi di ripristino.

3.3.2 Indisponibilità delle sedi operative

In caso di impossibilità ad accedere alle sedi:

- attivazione di sedi alternative o siti secondari individuati nel Piano;
  - DUC quarto piano (circa 50 postazioni) back office.
  - Centro unificato emergenze – protezione civile (circa 20 postazioni) back office.
  - Laboratori aperti (circa 50 postazioni) front office.
  - Biblioteca civica (circa 20 postazioni) front office.
- predisposizione di postazioni mobili o smart working per i servizi compatibili;
  - i notebook sono circa 700 il 50% delle postazioni di lavoro del Comune di Parma.
- coordinamento logistico per la fornitura di attrezzature e connettività;
  - la connettività è gestita dal fornitore dei servizi TLC (Retelit e Lepida).
- comunicazione al personale delle modalità operative temporanee.
  - Ufficio comunicazioni in collaborazione con il settore ITC.

3.3.3 Indisponibilità del personale

In caso di assenza prolungata o indisponibilità del personale chiave:

- attivazione di piani di sostituzione o delega;
- cross-training del personale per garantire la copertura dei ruoli critici;
- ricorso a supporto temporaneo di altre direzioni o fornitori esterni;
- aggiornamento dei referenti di processo per la redistribuzione delle attività.

3.3.4 Indisponibilità dei fornitori

In caso di interruzione dei servizi da parte di fornitori critici:

- attivazione di clausole contrattuali di continuità o disaster recovery;
- utilizzo di fornitori alternativi o soluzioni di backup;
- verifica del rispetto degli SLA e comunicazione tempestiva al BCM;
- aggiornamento del registro fornitori critici e revisione dei contratti in caso di criticità rilevate.

Per i fornitori critici sono previsti: due diligence basata sul rischio, referenti e sostituti reperibili, SLA coerenti con la BIA, procedure di escalation, obblighi di cooperazione e notifica a cascata, disponibilità di evidenze di test, continuità dei subfornitori e piani di uscita o soluzioni alternative. Le prestazioni durante test ed eventi reali sono monitorate e gli scostamenti sono gestiti come non conformità o rischio di terza parte.

4 MODALITA' DI COMUNICAZIONE

Le procedure di comunicazione sono necessarie al fine di attivare, in caso di accadimento di un evento di indisponibilità e/o di crisi, le opportune notifiche sia verso il personale interno all'azienda, sia verso gli stakeholder esterni.
Tutte le comunicazioni rilevanti devono essere:

- conservate secondo le procedure documentali del Comune;
- utilizzate per la valutazione post-evento;
- riesaminate in occasione dell'aggiornamento periodico del presente documento.

4.1 FLUSSI E CANALI DI COMUNICAZIONE

All'attivazione del Business Continuity Plan, il Responsabile della Continuità Operativa è tenuto ad avviare il flusso di comunicazione verso la Direzione e i Responsabili di Settore/Servizio interessati.
I canali primari che devono essere utilizzati sono il telefono e la posta elettronica istituzionale; in caso di indisponibilità, vengono previsti canali alternativi quali *Teams* o sistemi di messaggistica interna. Tutte le comunicazioni rilevanti devono essere tracciate e, ove necessario, formalizzate.
Nel caso di interruzione del servizio dovuta ad incidente Informatico, in quanto il Comune di Parma risulta *soggetto importante*, è necessario segnalare entro ventiquattro (24) ore gli incidenti indicati[1], e notificare entro settantadue (72) ore tutti gli elementi informativi disponibili al CSIRT Italia.
La segnalazione e la successiva notifica deve essere effettuata tramite la compilazione e l'invio di un modulo online apposito disponibile sul sito web del CSIRT Italia. [2]
Per ulteriori dettagli si rimanda alla procedura di gestione incidenti di sicurezza delle informazioni.

4.2 COMUNICAZIONI INTERNE

In caso di evento di indisponibilità e/o di crisi, la comunicazione verso l'interno deve essere effettuata dal BCM, con il supporto delle Risorse Umane, nella scelta del linguaggio e mezzo più consono.
La comunicazione interna è rivolta al personale interessato e ai soggetti coinvolti nella gestione dell'emergenza (dirigenti, responsabili di servizio, unità operative). I messaggi interni riguardano:

[1] https://www.acn.gov.it/portale/documents/d/guest/allegato-4-v2
[2] https://www.csirt.gov.it/segnalazione

- l'attivazione del Business Continuity Plan e il livello di emergenza;
- le istruzioni operative da seguire;
- l'eventuale riorganizzazione delle attività e delle sedi di lavoro;
- le misure di sicurezza e le modalità di contatto dei referenti.

Chi riceve la comunicazione è tenuto ad assicurare la diffusione delle informazioni al personale relativo alle proprie strutture e devono verificare la corretta attuazione delle indicazioni ricevute.
Gli aggiornamenti devono essere forniti con cadenza definita o al variare delle condizioni operative.

4.3 COMUNICAZIONI ESTERNE

La comunicazione esterna riguarda cittadini, fornitori, enti sovraordinati e autorità competenti ed ha come oggetto:

- eventuali disservizi o riduzioni dei servizi;
- servizi garantiti e modalità alternative di accesso;
- misure adottate dal Comune;
- tempi stimati di ripristino.

Relativamente alla comunicazione verso i cittadini, verranno utilizzati mezzi di stampa, tra cui TV Parma.
Per la comunicazione verso le autorità competenti, si utilizzeranno comunicati ufficiali.
Le comunicazioni esterne sono in carico all'Ufficio Comunicazione del Comune di Parma; qualora si tratti di scenari più gravi, verranno coinvolti il Sindaco e il Direttore Generale.
Infine, tutte le comunicazioni devono essere autorizzate e conformi alle disposizioni normative vigenti.

5 FORMAZIONE

Al fine di garantire l'attuazione e la corretta implementazione delle Strategie di Continuità e delle attività previste per la gestione della crisi, l'Ente si occuperà di coordinare un programma di awareness e formazione partendo dal personale coinvolto nel Processo di Business Continuity e arrivando fino a tutta la popolazione aziendale.
Le attività di sensibilizzazione devono comprendere la diffusione di informative interne, la pubblicazione della documentazione sulla intranet istituzionale e momenti informativi dedicati ai Responsabili di Settore e al personale coinvolto nei servizi essenziali.
L'obiettivo della formazione includerà la spiegazione dei principali elementi previsti nel Piano di Business Continuity.

6 MANTENIMENTO E REVISIONE DEL PIANO

Il mantenimento del Piano di Business Continuity garantisce che le strategie, le procedure e le responsabilità descritte restino efficaci e coerenti con l'evoluzione organizzativa, tecnologica e normativa del Comune.
L'obiettivo è assicurare che il Piano sia sempre aggiornato, accessibile e applicabile in caso di necessità, prevenendo l'obsolescenza delle informazioni e la perdita di efficacia operativa.

6.1 PERIODICITA' E CRITERI DI AGGIORNAMENTO

Il Piano deve essere sottoposto a riesame periodico e aggiornato ogniqualvolta si verifichino modifiche significative nei processi, nelle infrastrutture o nell'organizzazione.
Il riesame deve essere pianificato con cadenza almeno annuale o in occasione di uno dei seguenti eventi:

- aggiornamento o introduzione di nuovi servizi o processi critici;
- cambiamenti infrastrutturali o tecnologici che influenzano la capacità operativa (es. migrazione di data center, nuove soluzioni cloud, sostituzione di applicativi chiave);
- variazioni organizzative o di responsabilità (es. nuovi referenti, cambi di struttura o outsourcing di servizi);
- esito di test o simulazioni di continuità operativa, che evidenzino criticità o punti di miglioramento;
- eventi reali di crisi o interruzione che abbiano comportato l'attivazione, totale o parziale, del Piano.

Ogni aggiornamento deve essere documentato e tracciato, indicando le modifiche apportate, la motivazione e la data di rilascio della nuova versione.
Il programma di esercitazione deve coprire, con frequenza determinata dal rischio e almeno mediante un riesame annuale, scenari cyber e non cyber, indisponibilità di sedi, cloud, telecomunicazioni e fornitori. Sono misurati almeno tempi effettivi di attivazione e ripristino, perdita dati effettiva, successo delle procedure alternative, efficacia delle comunicazioni, disponibilità del personale e risposta dei fornitori. Scostamenti e carenze generano azioni correttive con responsabile, scadenza ed evidenza di chiusura, nonché aggiornamento di BIA, Registro dei Rischi, SoA e Piano di Trattamento/Adeguamento.

6.2 REGISTRO DELLE VERSIONI E RESPONSABILITA' DI REVISIONE

Tutte le modifiche al Piano devono essere registrate in un Registro delle versioni, che costituisce parte integrante del presente documento. Il registro consente di mantenere la tracciabilità delle revisioni e di assicurare che tutte le parti interessate dispongano della versione più aggiornata.
La responsabilità del mantenimento e della revisione del Piano è attribuita al Business Continuity Manager (BCM).

Il BCM è tenuto a:

- coordinare le attività di revisione e approvazione delle nuove versioni del Piano;
- garantire che i cambiamenti siano comunicati a tutti i destinatari del documento;
- archiviare le versioni precedenti per riferimento e audit;
- assicurare la coerenza tra il BCP e gli altri documenti di gestione della continuità e del rischio (es. DRP, BIA, ecc.).

Ogni nuova versione deve riportare in modo chiaro:

- il numero di versione e la data di rilascio;
- il soggetto che ha effettuato l'aggiornamento;
- la descrizione sintetica delle modifiche introdotte;
- il soggetto che ha approvato la nuova versione.

6.3 INTEGRAZIONE CON ALTRI PIANI

Il Piano di Business Continuity deve mantenere coerenza e integrazione con gli altri strumenti di pianificazione e gestione adottati dal Comune, in particolare:

- il Piano di Disaster Recovery, che disciplina le attività tecnico-infrastrutturali di ripristino dei sistemi informativi;
- la Business Impact Analysis (BIA), da cui il Piano trae le informazioni sui processi critici, i RTO e i RPO di riferimento;
- eventuali policy o procedure di risk management, compliance e sicurezza IT.

L’aggiornamento di uno di tali documenti deve determinare la verifica di coerenza e, se necessario, la revisione conseguente del BCP. In tal modo si garantisce una gestione integrata della continuità operativa e della resilienza complessiva del Comune.
I riferimenti incrociati obbligatori comprendono inoltre: CdP_Organizzazione per la sicurezza informatica – Ruoli e Responsabilità, CdP_Politica di sicurezza informatica e per la sicurezza delle informazioni, PR-SGSI-001, CdP_Piano di Adeguamento, POL-SGSI-018 Piano Disaster Recovery, CdP_Piano di gestione delle Crisi e CdP_Procedura di Gestione incidenti di sicurezza delle informazioni. La SoA deve indicare il presente Piano quale evidenza primaria per il controllo A.5.30 e per gli ulteriori controlli di continuità applicabili.

Comune di Parma

ALLEGATI
Schede di business impact analysis
Piano di Disaster Recovery
Elenco contatti di emergenza
Template di comunicazioni