Comune di Parma

PIANO DI DISASTER RECOVERY

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: 03/06/2026
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
Ferioli Nicola	Dirigente 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.

Sommario

GENERALITÀ E OBIETTIVO DEL DOCUMENTO ..... 7~~8~~

SCOPO DEL DOCUMENTO ..... 7~~8~~
VINCOLI E CONDIZIONI ..... 8~~9~~
MEMORIZZAZIONE E SUPPORTI RELATIVI AL PIANO ..... 9~~10~~

DESCRIZIONE DEL PERIMETRO DI ATTUAZIONE DEL DRP 10

SEDI AZIENDALI E DATA CENTER 10
INFRASTRUTTURA SISTEMI TECNOLOGICI 11
INFRASTRUTTURA DI RETE E CONNETTIVITÀ ..... 12~~13~~
INFRASTRUTTURA TECNOLOGICA DATA CENTER ..... 13~~14~~

INDIVIDUAZIONE DEGLI ATTORI ..... 14~~15~~

LIVELLI DI SERVIZIO ..... 15~~16~~

PARAMETRI DI RIFERIMENTO ..... 15~~16~~

PIANO DI DISASTER RECOVERY - PROCESSO DI ATTIVAZIONE E RIPRISTINO ..... 16~~17~~

CONTESTO ..... 16~~17~~
FASI DEL PIANO DI DISASTER RECOVERY ..... 18~~19~~
Valutazione della situazione di crisi o indisponibilità del sito primario ..... *18~~19~~*
Dichiarazione del disastro ..... *19~~20~~*
Notifica e attivazione delle strutture coinvolte ..... *19~~20~~*
Attivazione del Piano di DR e delle procedure ad esso connesse ..... *19~~20~~*
Attivazione del sito remoto di DR e avvio delle operazioni di ripristino ..... *20~~21~~*
Ripristino dei sistemi presso il sito di DR ..... *20~~21~~*
Comunicazione relativa al completamento del processo di ripristino ..... *22~~23~~*
Ripristino del sito primario e "Dichiarazione di fine emergenza" ..... *22~~23~~*
Analisi post-evento e miglioramento continuo ..... *23~~24~~*

TEST DELL'INFRASTRUTTURA E DEL PIANO ..... 23~~24~~

SPECIFICA DELLA METODOLOGIA ADOTTATA ..... 23~~24~~
SPECIFICHE RELATIVE ALLA INDIVIDUAZIONE DELLA FINESTRA TEMPORALE ..... 23~~24~~
PIANIFICAZIONE DEL TEST ..... 24~~25~~
DEBRIEFING E RAPPORTO FINALE DI TEST ..... 24~~25~~

MANUTENZIONE DEL PIANO DI DISASTER RECOVERY ..... 24~~25~~

EVENTI CHE PREVEDONO IL RIESAME ..... 25~~26~~
PROCESSO DI CHANGE ..... 25~~26~~
Segnalazione evento ..... *26~~27~~*
Verifica impatti ..... *26~~27~~*
Esecuzione change ..... *26~~27~~*

FORMAZIONE ..... 27~~28~~

ALLEGATI ..... 27~~28~~

SCHEDE DI BUSINESS IMPACT ANALYSIS ..... 27~~28~~
BUSINESS CONTINUITY PLAN ..... 27~~28~~
ORGANIZZAZIONE PER LA SICUREZZA INFORMATICA - RUOLI E RESPONSABILITA' PER LA GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI ..... 27~~28~~

ACRONIMI E DEFINIZIONI

Acronimo	Definizione
DR	Disaster Recovery Plan
DRM	Disaster Recovery Manager
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.
SLA	*Service Leve Agreement*

RIFERIMENTI NORMATIVI

Di seguito sono riportati i principali riferimenti normativi che hanno guidato la redazione del presente documento:

Regolamento (UE) 2016/679 - GDPR: regolamento europeo che stabilisce norme per la protezione dei dati personali e la sicurezza del trattamento, imponendo misure di resilienza e disponibilità dei sistemi (art. 32).

NIST SP 800-34 Rev.1 - "Contingency Planning Guide for Federal Information Systems": guida di riferimento per la pianificazione e lo sviluppo dei piani di contingenza e di ripristino dei sistemi informativi.

ISO 22301:2019 - "Security and resilience - Business continuity management systems - Requirements": standard internazionale che definisce i requisiti per l'implementazione di un Sistema di Gestione della Continuità Operativa (BCMS).

NIST SP 800-53 Rev.5 - "Security and Privacy Controls for Information Systems and Organizations": guida del NIST per la gestione della sicurezza informatica, che include controlli di sicurezza e di continuità operativa.

Cloud Security Alliance (CSA) - Cloud Control Matrix (CCM v4): framework che fornisce una serie di controlli di sicurezza per la gestione dei rischi associati ai fornitori di servizi cloud.

ISO 22317:2021 - "Security and resilience - Guidelines for business impact analysis (BIA)": linee guida per la conduzione della Business Impact Analysis (BIA), utili a definire priorità e tempi di ripristino.

ISO/IEC 27001:2022 - "Information Security Management Systems (ISMS)": norma internazionale che specifica i requisiti per un sistema di gestione della sicurezza delle informazioni (ISMS), includendo anche i controlli sulla continuità operativa.

Direttiva (UE) 2022/2555 - NIS2: aggiorna e sostituisce la Direttiva NIS, rafforzando gli obblighi di sicurezza, resilienza e continuità per le amministrazioni pubbliche e i soggetti essenziali.

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: A.5.23 sicurezza nell'uso dei servizi cloud; A.5.30 prontezza ICT per la continuità operativa; A.8.9 gestione della configurazione; A.8.16 attività di monitoraggio.
PR-SGSI-001 – Processo di Valutazione e trattamento del rischio, Business Impact Analysis, Registro dei Rischi, Piano di Trattamento del Rischio e Dichiarazione di Applicabilità (SoA), nelle versioni vigenti.
SOC 2 (System and Organization Controls 2): framework di assurance che definisce i criteri di sicurezza, disponibilità, integrità dei processi, riservatezza e privacy per le organizzazioni che trattano dati sensibili.

D.Lgs. 36/2023 - Nuovo Codice dei Contratti Pubblici: prevede che i fornitori ICT assicurino requisiti di sicurezza, continuità e recupero dati nei contratti di servizio con le Pubbliche Amministrazioni.

Agenzia per l'Italia Digitale (AgID) - "Linee Guida per il Disaster Recovery delle Pubbliche Amministrazioni": documento ufficiale che fornisce indicazioni per la predisposizione e la gestione dei piani di DR delle Pubbliche Amministrazioni, in attuazione dell'art. 50-bis del CAD.

NIST Cybersecurity Framework 2.0 (2024): versione aggiornata del framework NIST che include la nuova funzione Govern e potenzia la funzione Recover, con un focus esteso sulla resilienza operativa e sulla gestione integrata del rischio.

Circolari e Linee Guida dell'Agenzia per la Cybersicurezza Nazionale (ACN) (2024): forniscono indicazioni operative per la gestione degli incidenti, la resilienza informatica e l'allineamento delle PA agli standard NIST e ISO.

Contratto di servizio in vigore fino ad aprile 2028 Rep. SP/20365/2025 del 4 luglio 2025, che nomina It.City Gestore del Sistema Informatico Comunale di Parma.

Modello di Organizzazione, Gestione e Controllo ex D. lgs. 231/2001 della Società IT.City S.p.A. a socio unico

Misure di sicurezza ITC, in attuazione della Direttiva 1° agosto 2015 del Presidente del Consiglio dei Ministri, elencate nella circolare AGID del 18 aprile 2017, n. 2/2017.

Codice dell'amministrazione digitale - testo unico che riunisce e organizza le norme riguardanti l'informatizzazione della Pubblica Amministrazione nei rapporti con i cittadini e le imprese. Istituito con il decreto legislativo 7 marzo 2005, n. 82, successivamente modificato e integrato prima con il decreto legislativo 22 agosto 2016 n. 179 e poi con il decreto legislativo 13 dicembre 2017 n. 217) **Articolo 51.** Sicurezza dei dati, dei sistemi e delle infrastrutture delle pubbliche amministrazioni

Sistema di Gestione della Sicurezza delle Informazioni (SGSI) di IT.City S.p.A. a socio unico

GENERALITÀ E OBIETTIVO DEL DOCUMENTO

SCOPO 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-018 "Piano di DIsaster Recovery",. Restano in capo al Comune le funzioni di indirizzo, approvazione, supervisione, vigilanza e governo del rischio.
Il presente documento definisce l'insieme delle misure, dei processi organizzativi e delle procedure tecniche finalizzate a garantire la ripartenza dei servizi informatici critici del Comune di Parma a seguito di eventi di natura disastrosa che ne determinino l'interruzione o una riduzione significativa della disponibilità o delle prestazioni operative.
Il piano si applica all'intero ambiente ICT gestito da IT.CITY per conto del Comune di Parma e ha lo scopo di:

- assicurare la continuità dei servizi IT essenziali per il funzionamento dell'Amministrazione e per l'erogazione dei servizi ai cittadini;
- definire le responsabilità e le procedure operative da attuare in caso di indisponibilità dei sistemi primari;
- garantire il ripristino dei sistemi informativi e delle infrastrutture nei tempi compatibili con i livelli di servizio concordati (RTO/RPO);

- mantenere la conformità normativa alle disposizioni vigenti in materia di sicurezza delle informazioni e protezione dei dati personali.

Il Disaster Recovery Plan (di seguito, anche: "DRP") è parte integrante del Piano di Business Continuity (BCP) e ne rappresenta la componente tecnica dedicata alla gestione delle attività di ripristino ICT.
Mentre il BCP disciplina l'organizzazione complessiva della risposta e le modalità di mantenimento della continuità dei servizi essenziali, il DRP si focalizza sugli aspetti tecnologici e infrastrutturali, necessari per ristabilire l'operatività dei sistemi informativi che supportano i processi critici.
Il DRP si integra con:
Il Piano costituisce evidenza operativa del controllo ISO/IEC 27002:2022 A.5.30 ed è gestito nel ciclo del SGSI: il contesto e le dipendenze sono definiti nella BIA e nel risk assessment; le strategie sono selezionate nel trattamento del rischio e tracciate nella SoA; test, incidenti, scostamenti e non conformità alimentano monitoraggio, riesame e miglioramento secondo le clausole 4-10 della ISO/IEC 27001:2022.

- la Business Impact Analysis (BIA), che identifica i processi critici e i requisiti di ripristino;
- le policy di sicurezza ICT e privacy di IT.CITY e del Comune di Parma;
- i contratti di servizio stipulati con i fornitori tecnologici (es. Lepida S.c.p.A) che gestiscono data center, rete e connettività.

VINCOLI E CONDIZIONI

L'efficacia e l'applicabilità del presente piano dipendono dal rispetto di una serie di vincoli di natura infrastrutturale, organizzativa, contrattuale e normativa, che garantiscono la possibilità di attuare correttamente le procedure di ripristino previste. Prima di illustrarli, si riportano alcuni concetti di riferimento utili a definire l'ambito di attivazione del piano.
Il sistema informativo del Comune di Parma è considerato affetto da un evento disastroso qualora si verifichino circostanze tali da rendere impossibile o gravemente compromessa la normale erogazione dei servizi informatici critici.
Le principali caratteristiche di un evento disastroso sono:

- **Degradazione del servizio**, quando l'evento causa o può causare, nel breve o medio periodo, una riduzione significativa della capacità di erogare i servizi informatici essenziali (ad esempio, l'indisponibilità dell'infrastruttura per un periodo superiore ai valori di RTO previsti, tale da richiedere l'attivazione del DRP);
- **Irreversibilità**, quando l'evento impedisce il ripristino dei sistemi nel sito primario entro tempi compatibili con le esigenze operative e con i livelli di servizio concordati (RTO/RPO).

Il verificarsi di una di tali condizioni costituisce la soglia di attivazione del piano, la cui efficacia è comunque subordinata a una serie di vincoli infrastrutturali, organizzativi e contrattuali.
Dal punto di vista infrastrutturale, il piano si applica all'ambiente ICT gestito da IT.CITY per conto del Comune di Parma, basato su infrastrutture fornite da Lepida S.c.p.A. in configurazione di alta affidabilità, comprendenti un data center primario e un sito secondario. L'attuazione delle procedure di ripristino presuppone la disponibilità del sito alternativo e la piena funzionalità dei sistemi di replica e dei meccanismi di backup off-site.
Sotto il profilo organizzativo, il DRP è vincolato alla disponibilità minima delle risorse umane necessarie per l'attivazione e la gestione delle procedure di recupero. La sua efficacia dipende inoltre dall'esistenza di processi formalmente approvati per la gestione delle emergenze ICT e dall'allineamento costante tra le procedure operative e l'evoluzione dell'infrastruttura tecnologica.

In termini contrattuali, l'efficacia del piano dipende dal rispetto degli accordi di servizio vigenti tra Comune, IT.CITY e fornitori. I tempi di intervento, la disponibilità dei sistemi e i limiti di perdita dei dati devono risultare coerenti con i parametri definiti nei Service Level Agreement (SLA), che rappresentano la base di riferimento per la determinazione degli RTO e degli RPO dei singoli servizi.
Per i servizi cloud, IaaS, SaaS e per gli altri fornitori critici, il Comune mantiene la responsabilità di governo e verifica. Contratti e accordi operativi devono includere responsabilità condivise, requisiti di backup e ripristino, RTO/RPO coerenti con la BIA, sicurezza e localizzazione delle copie, portabilità ed esportabilità dei dati, supporto in emergenza, continuità dei subfornitori, obblighi di notifica a cascata, partecipazione ai test, restituzione delle evidenze e strategia di uscita.
Di seguito vengono presentati gli scenari di crisi rispetto ai quali il piano garantisce la capacità di ripristino dei servizi informatici critici. La copertura dei requisiti definiti per tali scenari è limitata, nell'ambito del presente piano, alla sola erogazione dei servizi ICT oggetto del documento.
Gli scenari di riferimento, individuati sulla base del documento di Business Impact Analysis (BIA), sono i seguenti:

1. distruzione o inaccessibilità di strutture nelle quali sono allocate unità operative o apparecchiature critiche;
2. indisponibilità di sistemi informativi critici, anche con riferimento ai sistemi funzionali alla prestazione dei servizi;
3. indisponibilità di personale essenziale per il funzionamento dei processi aziendali;
4. interruzione del funzionamento delle infrastrutture (tra cui, a titolo esemplificativo ma di certo non esaustivo: energia elettrica, reti di telecomunicazione, ecc.);
5. alterazione o perdita di dati e documenti critici;
6. Danneggiamenti gravi provocati dai collaboratori.

L'attuazione del piano è subordinata alla disponibilità delle figure operative e decisionali previste (Disaster Recovery Manager, Comitato di Crisi, team tecnici e referenti comunali). In caso di indisponibilità totale o parziale di tali figure, l'attuazione potrà essere adattata sotto la supervisione delle autorità competenti, nel rispetto delle priorità operative definite internamente e delle esigenze di continuità dei servizi essenziali.
Eventuali modifiche infrastrutturali, variazioni contrattuali o riorganizzazioni interne devono essere comunicate al Disaster Recovery Manager, che provvederà all'aggiornamento del piano secondo il processo di change management descritto nel Capitolo 7. Un riesame periodico dei vincoli, delle condizioni operative e degli scenari di crisi garantisce la coerenza tra la versione in vigore del DRP e lo stato effettivo dei sistemi e dei servizi ICT.

MEMORIZZAZIONE E SUPPORTI RELATIVI AL PIANO

Il DRP è gestito e conservato in formato elettronico, con l'obiettivo di garantirne l'integrità, la riservatezza e la disponibilità anche in condizioni di emergenza.
Modalità di gestione e conservazione:

- Il documento è archiviato nel repository documentale di IT.CITY, in area riservata ai soggetti autorizzati (DR Manager, membri del Comitato di Crisi, referenti operativi);
- È conservata una copia di sicurezza presso il sito secondario (data center Lepida) per consentirne la consultazione anche in caso di indisponibilità del sito primario;
- Ogni revisione del documento è tracciata in un registro delle versioni, con data, autore della modifica, approvazione e descrizione sintetica dei cambiamenti effettuati;

- La distribuzione controllata del piano è effettuata dal DR Manager, che ne assicura la diffusione alle sole funzioni coinvolte e ne mantiene evidenza tramite apposito registro;
- Una verifica annuale del piano, o successiva a incidenti/test significativi, garantisce la coerenza tra la versione in vigore e lo stato effettivo dell'infrastruttura e dei servizi.

La responsabilità ultima della custodia e dell'aggiornamento del documento è in capo al Disaster Recovery Manager, che garantisce la disponibilità del piano in ogni momento utile all'attivazione delle procedure di emergenza.

DESCRIZIONE DEL PERIMETRO DI ATTUAZIONE DEL DRP

Il presente capitolo descrive il perimetro infrastrutturale, i siti, le modalità operative e gli strumenti tecnologici che vincolano e definiscono le attività del Piano di Disaster Recovery.

SEDI AZIENDALI E DATA CENTER

I principali siti aziendali all'interno dei quali sono ospitate le postazioni di lavoro dei dipendenti di IT.CITY e del Comune di Parma, che contribuiscono all'erogazione dei servizi e accedono ai dati strutturati (database) e ai dati non strutturati (es. documenti office) ospitati nell'infrastruttura tecnologica, sono:

LOCALIZZAZIONE GEOGRAFICA DEI SITI AZIENDALI		
GRUPPO	SOCIETA'	LOCALIZZAZIONE
Gruppo Parma	**IT.CITY SPA**	Largo Torello de Strada 15/A – Parma
Comune di Parma	**Direzionale Uffici Comunali**	Largo Torello de Strada 11/A – Parma
Comune di Parma	**Sede Municipale**	Strada della Repubblica, 1 – Parma
Comune di Parma	**Centro unificato delle emergenze**	Strada del Taglio 8/a – Parma
Comune di Parma	**Sedi Secondarie (poli, scuole materne, biblioteche,etc.)**	All'interno dei confini comunali

L'infrastruttura tecnologica gestita da IT.CITY erogata da LEPIDA in modalità IaaS è la seguente:

TABELLA DATACENTER		
SOCIETA'	INDIRIZZO	UNITA' ORGANIZZATIVE
LEPIDA SCPA	Largo Torello de Strada 15/A - Parma	**Data Center primario** Datacenter (TIER 3) gestiti da Lepida, accesso solo su appuntamento e accompagnati da un tecnico Lepida sempre presente in fase di configurazione; area coperta da sistemi di videosorveglianza, di allarme antiintrusione e di controllo accessi
LEPIDA SCPA	Via Stefano Trenti, 39/1 - Ferrara	**Data Center remoto** Datacenter (TIER 3) gestiti da Lepida, accesso solo su appuntamento e accompagnati da un tecnico Lepida sempre presente in fase di configurazione; area coperta da sistemi di videosorveglianza, di allarme antiintrusione e di controllo accessi

INFRASTRUTTURA SISTEMI TECNOLOGICI

I sistemi tecnologici (server e postazioni di lavoro) sono configurati secondo procedure interne (governance ISO27001) che ne garantiscono la conformità rispetto alla normativa vigente in termini di sicurezza, disponibilità e performance. Sinteticamente:

Le configurazioni necessarie al ripristino devono essere gestite secondo il controllo A.8.9: baseline approvate e versionate, inventario delle dipendenze, copie protette delle configurazioni di rete e sicurezza, procedure di build e hardening, controllo delle modifiche e verifica periodica della corrispondenza tra configurazione documentata e ambiente effettivo. Le credenziali e le chiavi di emergenza sono custodite con accesso ristretto e procedure di utilizzo tracciate.

TABELLA DELLE COMPONENTI SW dei SISTEMI TECNOLOGICI	
SISTEMA	SW
Server Windows	Domain Controller MSSQL Server IIS Netwrix WSUS Gestionale Applicazioni Microsoft Office File server Terminal server Printer Server Alcatel telefonia
Server Open Source	Apache Tomcat Java ORACLE Sistemi di monitoraggio
Postazioni di lavoro IT.CITY	Applicazioni Microsoft Office Endpoint security protection Browser Acrobat Reader Software commesse (sviluppato internamente) CMDBuild (content management database) Presenze Visual Studio / Visual Studio Code GitHub Microsoft SQL Server Management Studio Client Oracle Sqldeveloper CommVault Simpana Putty KeyPass

TABELLA DELLE COMPONENTI SW dei SISTEMI TECNOLOGICI	
SISTEMA	SW
Postazioni di lavoro Comune di Parma	Applicazioni Microsoft Office Endpoint security protection Browser Acrobat Reader Client Oracle Arc Reader Software firma digitale

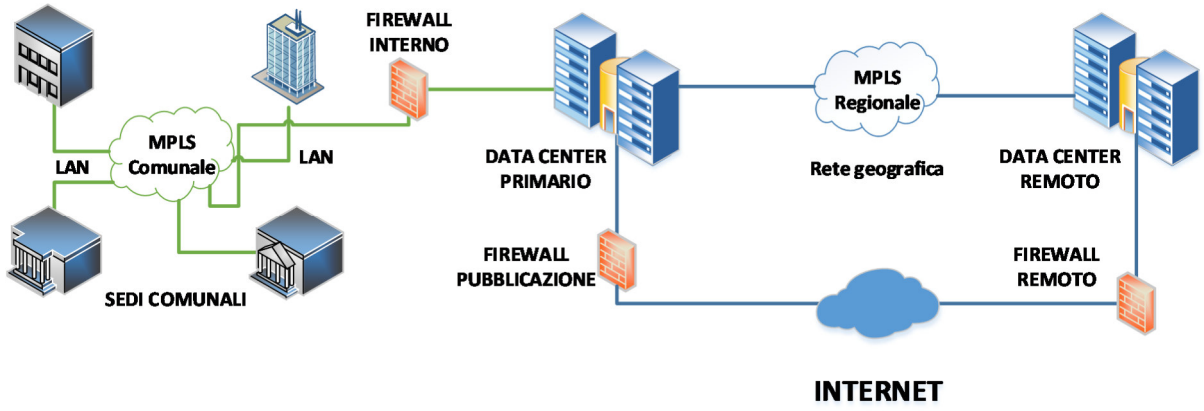
Le informazioni riguardanti i Server, i File System e VM utilizzati da ItCity e Comune di Parma sono riportate nell'allegato di dettaglio.

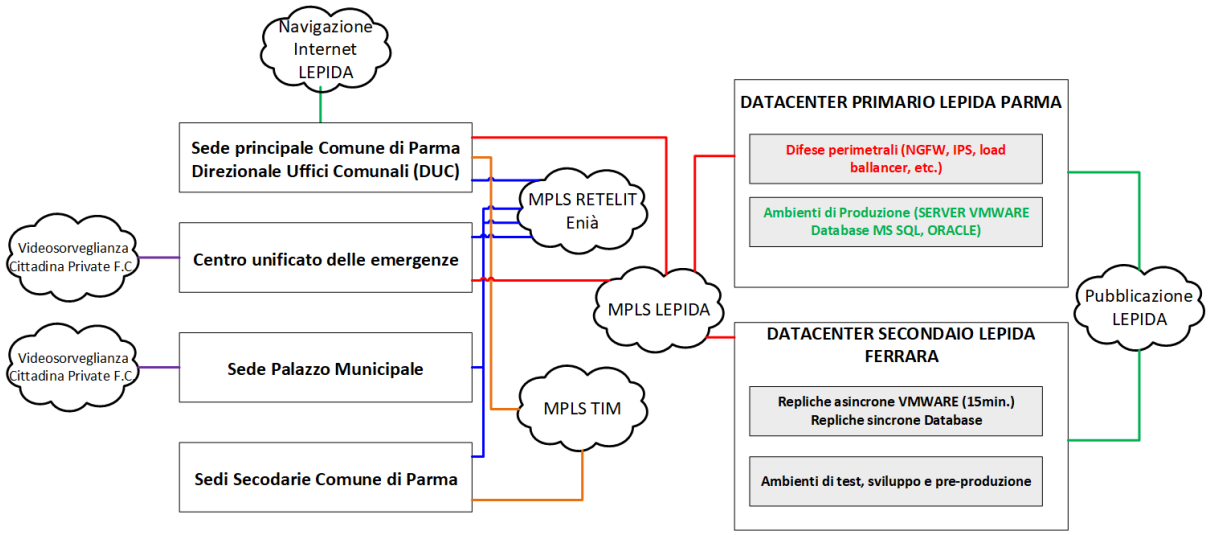
INFRASTRUTTURA DI RETE E CONNETTIVITÀ

Le sedi di IT.CITY e del Comune di Parma sono collegate tra loro tramite una rete MPLS (Multiprotocol Label Switching) gestita da RETELIT per le sedi principali e da TIM per le sedi secondarie.
La connettività fra i datacenter è gestita tramite una rete MPLS regionale.
Le due reti MPLS sono collegate tramite due punti d'accesso configurati in alta affidabilità ospitati nei locali tecnici della sede del Comune DUC-A e nella sede DUC-B.
Di seguito si riporta il dettaglio con la localizzazione e le funzioni:

LOCALI TECNICI ACCESSO MPLS		
LOCALE	LOCALIZZAZIONE	FUNZIONI
DUC-A	Largo Torello de Strada 15/A – Parma	Accesso principale da/verso datacenter e Accesso MPLS cittadina
DUC-B	Largo Torello de Strada 11/A – Parma	Accesso secondario da/verso datacenter e MPLS cittadina

Il traffico dati fra le reti MPLS è regolato da sistemi next generation firewall (NGFW) FORTINET FORTIGATE 1100 connessi in cluster in modalità *active-passive*
L'accesso a internet degli utenti è controllato dai NGFW.
La pubblicazione dei servizi è gestita da un sistema firewall HUAWEI interno ai datacenters. (principale e secondario), come da grafico sotto riportato.





INFRASTRUTTURA TECNOLOGICA DATA CENTER

Di seguito vengono riportate le caratteristiche specifiche dell'infrastruttura tecnologica (data center primario e secondario) e le configurazioni tecniche di replica che vincolano le attività del DRP.

- Ambienti virtuali: le macchine virtuali VMware sono replicate ogni 15min sul sito secondario tramite il sistema "site recovery", composto di due appliance (vSphere replication management server): uno sul sito primario e uno sul sito remoto. Le macchine virtuali sono emulazioni di computer fisici e forniscono capacità di funzionamento continuo senza guasti.
- Dati non strutturati: i documenti non strutturati (es. Office, CAD, etc.) ospitati sul servizio denominato "Nuvola" risiedono su apparati di Lepida SpA. La replica dei dati (asincrona) è inclusa nel servizio stesso ed è indicativamente di 15 min.
- Database Oracle: il software di replica Data Guard (copia sincrona) per l'ambiente database Oracle è gestita tramite il software di management Oracle Cloud Control, che fornisce un'intuitiva interfaccia utente per la configurazione del prodotto. La console Oracle Cloud verifica in tempo reale le prestazioni, gli spazi occupati, gli allarmi e gli errori, e consente la creazione di report automatici che possono essere inviati ai referenti per la gestione di potenziali incidenti. I dati dei database sono allineati in real-time su un'infrastruttura Oracle di stand-by che è ospitata all'interno dell'ambiente virtuale del sito di disaster recovery, analogamente a quanto predisposto per le macchine virtuali, e possono essere acceduti in sola lettura, in qualsiasi momento. La commutazione (fail-over) dal database principale a quello di stand-by può essere gestita in modalità manuale o automatica a seconda delle esigenze.
- Database Microsoft SQL Server: La replica per l'ambiente database Microsoft SQL è gestita tramite la tecnica di copia sincrona "log shipping" (real-time). I dati dei database sono allineati su un'infrastruttura di stand-by che è ospitata all'interno dell'ambiente virtuale del sito di disaster recovery e non possono essere acceduti se non a fronte del fail-over (manuale o automatico) dal database principale a quello di stand-by.
- Rete dati: Sono presenti tre differenti tipologie di rete dati:
    - Internet: connettività utilizzata sia per la navigazione dei dipendenti che per la pubblicazione dei servizi web. In entrambi i casi la continuità è garantita da Lepida,

in modalità “alta affidabilità” sia sui due data center per le linee di pubblicazione, sia sui due palazzi DUC A/B per la navigazione.
    - Reti locali: connettività delle postazioni di lavoro e connettività data center. La prima in gestione a Retelit non prevede sistemi ridondati, in caso di guasto di un apparato il presidio lo sostituisce entro il giorno successivo, la seconda in gestione a Lepida configurata in alta affidabilità.
    - Reti geografiche: rete MPLS per la connettività delle sedi comunali e rete regionale per la connettività data center. La prima in gestione a Retelit per le sedi principali (DUC, Municipio, Polizia Locale) in alta affidabilità (sono previste linee di backup) e TIM per le sedi secondarie (Poli sociali, biblioteche, etc.) NON in alta affidabilità (in caso di guasto deve intervenire un tecnico TIM). La connettività regionale è gestita da Lepida ed è progettata in alta affidabilità tramite diversi percorsi in fibra su canalizzazioni separate.
- Sistemi di difesa perimetrali: sono presenti due tipologie
    - Firewall: la continuità operativa del servizio firewall dei due data center richiede un intervento tecnico da parte di Lepida (da inserire nella tabella ruoli/responsabilità). Il servizio firewall per il controllo della navigazione degli utenti è configurato in alta affidabilità con commutazione automatica, non richiede un intervento di un operatore
    - Reverse proxy: il servizio di pubblicazione è configurato in alta affidabilità con commutazione automatica, non richiede un intervento di un operatore.

INDIVIDUAZIONE DEGLI ATTORI

Per garantire un’attivazione efficace e coordinata del Piano di Disaster Recovery, il Comune di Parma si avvale di una struttura organizzativa dedicata, composta da ruoli e responsabilità definite.
Gli Organi di Amministrazione e Direttivi approvano le modalità di implementazione del DRP e ne sovrintendono l’efficacia sulla base di report relativi a test, RTO/RPO effettivi, rischi residui e azioni correttive. Il RTD assicura il raccordo con il SGSI e con il Piano di Business Continuity; il DRM coordina le attività tecniche.

• **Disaster Recovery Manager (DRM)**
Responsabile del coordinamento generale delle attività di ripristino, della dichiarazione di disastro (previa autorizzazione del Comitato di Crisi) e della comunicazione ufficiale sugli avanzamenti.
Owner: Comune di Parma
• **Comitato di crisi**
È il principale organo decisionale durante un’emergenza. Valuta l’impatto dell’evento, dichiara lo stato di crisi e approva l’attivazione del Piano di DR. Coordina le comunicazioni istituzionali, definisce le priorità di intervento e autorizza eventuali risorse straordinarie.
Owner: Comune di Parma
• **Team tecnico**
Esegue gli interventi tecnici previsti dal piano, incluse analisi dei guasti, restore, avvio dei sistemi in ambiente di DR e rientro in produzione. Monitora lo stato delle infrastrutture, segnala criticità al Referente DR e collabora con i fornitori esterni per attività specialistiche.
Owner: IT.CITY
• **Fornitori esterni**

Supportano le attività di ripristino mettendo a disposizione servizi, competenze e tecnologie (es. hosting, network, sicurezza, hardware). Garantiscono i livelli di servizio (SLA) previsti nei contratti e forniscono assistenza tecnica per tutta la durata dell'emergenza.

• **Referenti funzionali**

Rappresentano gli uffici e le aree operative dell'Amministrazione. Indicano le priorità dei servizi, verificano l'impatto sul territorio e partecipano alla fase di test e validazione degli applicativi ripristinati. Comunicano esigenze specifiche al Comitato di Crisi e al Referente DR.

Owner: Comune di Parma

LIVELLI DI SERVIZIO

Il presente capitolo definisce i livelli di servizio (Service Level Agreement - SLA) del Piano di Disaster Recovery del Comune di Parma, intesi come obiettivi di ripristino che orientano le attività operative e organizzative da attuare in caso di interruzione dei sistemi informativi.

Gli SLA rappresentano i valori di riferimento derivanti dalla Business Impact Analysis (BIA) e consentono di determinare:

- i tempi massimi di inattività tollerabili per ciascun servizio (RTO - Recovery Time Objective);
- la quantità massima di dati potenzialmente perdibili senza compromettere la continuità operativa (RPO - Recovery Point Objective).

Questi parametri costituiscono la base per pianificare le strategie di recupero e definire l'ordine di priorità dei servizi e delle infrastrutture da ripristinare.

RTO e RPO non sono determinati esclusivamente dagli SLA del fornitore: devono derivare dalla BIA, risultare compatibili con il tempo massimo tollerabile di interruzione e con il livello minimo di servizio, essere approvati dai responsabili di processo e verificati mediante test. Eventuali disallineamenti tra requisiti dell'Ente e capacità tecniche o contrattuali sono registrati nel Registro dei Rischi e nel Piano di Adeguamento.

PARAMETRI DI RIFERIMENTO

In caso di disservizio, i parametri da considerare sono:

- RTO (Recovery Time Objective): tempo massimo entro il quale un servizio o sistema deve essere ripristinato per evitare impatti critici sull'operatività.
- RPO (Recovery Point Objective): intervallo massimo di perdita dati accettabile, misurato come tempo trascorso dall'ultimo backup valido.

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

- TMA (Tempo Massimo di Attivazione del Piano): intervallo entro il quale deve essere operativo il team di Disaster Recovery e avviate le prime azioni di ripristino.

Il TMA deve essere definito in modo da garantire la tempestiva attivazione del Piano e la disponibilità delle risorse necessarie per l'avvio delle operazioni di ripristino. Al momento dell'attivazione, i referenti e i membri del team devono essere contattati senza ritardo e, in caso di indisponibilità, devono essere attivati i sostituti designati. Tutti i componenti del team devono essere contattati immediatamente al momento dell'attivazione.
Il rispetto dei livelli di servizio viene verificato periodicamente tramite test di ripristino, esercitazioni e controlli programmati. L'aggiornamento dei parametri SLA deve avvenire ogniqualvolta intervengano modifiche significative nei:

- servizi ICT;
- infrastrutture tecnologiche;
- sistemi applicativi o procedure operative.

Il mantenimento degli SLA garantisce al Comune di Parma la tempestiva ripresa dei servizi pubblici essenziali e livelli adeguati di disponibilità, affidabilità e continuità operativa.

PIANO DI DISASTER RECOVERY - PROCESSO DI ATTIVAZIONE E RIPRISTINO

CONTESTO

Il processo decisionale che ha guidato la definizione del Piano di Disaster Recovery ha tenuto conto dei seguenti elementi:

- Possibilità di attivare sia soluzioni "offline" che soluzioni "online";
- Tempi di realizzazione;
- flessibilità della soluzione.

La soluzione "offline" prevede il ripristino utilizzando le copie di sicurezza offline (backup). Gli elementi a sfavore di tale soluzione sono soprattutto i tempi di ripristino, oltre a possibili perdite di dati in relazione alle politiche di retention del processo di backup. I sistemi di backup, in tipologia DDT (disk-disk-tape), sono da considerarsi infrastruttura di ripristino esclusivamente in caso di evento disastroso capace di inibire il funzionamento sia del DC primario che del DC secondario (evento altamente improbabile). I backup sono generalmente utilizzati per recuperare i dati in caso di "disastro" parziale (es. cancellazioni involontarie). Dobbiamo sottolineare che in caso di evento disastroso i tempi di ripristino oltre le attività di *restore* dai nastri magnetici devono tener conto dei tempi di approvvigionamento dell'hardware in carico a Lepida.
Le copie destinate al cyber recovery devono essere separate logicamente o fisicamente dagli ambienti di produzione, protette da modifica e cancellazione non autorizzata, cifrate ove appropriato, soggette a retention approvata e accessibili mediante privilegi distinti. Replica e alta affidabilità non sostituiscono il backup: devono essere previste prove periodiche di leggibilità e ripristino, verifiche di integrità e procedure per evitare che malware, ransomware o corruzione dei dati si propaghino alle copie di recupero.

La soluzione "online" consiste sostanzialmente nella replica *real-time* (sincronizzazione continua) degli ambienti virtuali e dei database relazionali dal sito primario al sito remoto. Il piano (tempi e costi) di "disaster recovery" per il Comune di Parma, fra il Datacenter Lepida Parma e il Datacenter Lepida Ferrara, prevede una configurazione *active/passive* su connettività Layer 2. Tale configurazione, prevede l'installazione degli ambienti di produzione sul sito primario e la copia offline sul sito remoto. Il sito remoto, in funzionamento "normale", è utilizzato per l'erogazione degli ambienti di test/preproduzione che in caso di disastro devono essere spenti per liberare le risorse necessarie per l'attivazione delle "repliche".

Il piano di Disaster Recovery progettato consente la riattivazione dei servizi *"core"* entro 8/10 ore dalla sua attivazione.
Il rientro sul sito primario, una volta risolto il "disastro", richiede diversi giorni di lavoro, per tale motivo l'attivazione del piano di Disater Recovery deve essere valutata con attenzione per evitare disservizi maggiori di quanto il disastro stesso possa causare.

Il piano di DR è composto di Informazioni Statiche: informazioni che rimarranno costanti e non saranno oggetto di frequente revisione) e Informazioni Dinamiche: informazioni che necessitano di un regolare e costante aggiornamento per provvedere al corretto mantenimento del piano stesso.
Rientrano nelle informazioni statiche
Dati strutturali. Informazioni relative agli stabili che ospitano sia l'ente sia i sistemi di elaborazione (Data Center). Si precisa che il sito primario risulta, sotto il profilo prevenzionistico, essere conforme alle vigenti disposizioni in materia di igiene e sicurezza sul lavoro (D. Lgs. 81/2008) e di prevenzione incendi (DPR 157/2011 – D.M. 10/03/98).
Alimentazione Elettrica. Gruppi di continuità elettrica (UPS).
Sistemi antincendio delle sedi degli uffici e nel Data Center.
Sistemi antintrusione delle sedi degli uffici e nel Data Center.
Aree di emergenza. locali attrezzati dove sistemare i dipendenti in caso di parziale inagibilità degli uffici.

Il Piano trova applicazione in caso di eventi che comportino l'indisponibilità dei sistemi informativi dell'Ente.
Di seguito i principali rischi considerati:

- mancanza di erogazione dei servizi del Data Center dovuta all'impossibilità di accedere ai dati o alle banche dati;
- Distruzione o danneggiamento grave delle infrastrutture IT o del Data Center, tale da compromettere l'erogazione dei servizi informatici e non risolvibile entro i tempi massimi di inattività definiti nella Business Impact Analysis (BIA) e nel Piano di Continuità Operativa (BCP).

Sono invece esclusi dal perimetro del presente Piano i seguenti scenari:

- indisponibilità contemporanea dei siti primario e secondario;
- perdita simultanea dei dati presenti in entrambi i siti.

L'esclusione operativa degli scenari di indisponibilità simultanea dei siti o perdita delle copie non equivale ad accettazione implicita. Tali scenari devono essere valutati nella procedura PR-SGSI-001; il rischio residuo deve essere formalmente trattato o accettato dagli organi competenti e, ove la protezione risulti insufficiente, deve essere aperta un'azione nel Piano di Adeguamento, ad esempio per copie offline/immutabili, sito o deposito alternativo e procedure di ricostruzione controllata.

Ambiti di competenza e perimetro tecnico del Piano

Il Piano di Disaster Recovery si basa su un'infrastruttura e su un modello organizzativo che coinvolgono diversi soggetti, ciascuno con competenze specifiche sui vari livelli del sistema informativo comunale.

La seguente tabella descrive i principali ambiti di competenza tecnica e gestionale che rientrano nel perimetro di applicazione del Piano, indicando per ciascun ambito il soggetto titolare e il relativo ruolo di presidio. Questa rappresentazione ha lo scopo di definire i confini tecnici e operativi entro i quali il Piano di Disaster Recovery viene attuato, chiarendo le interdipendenze tra Comune di Parma, Lepida S.c.p.A., IT City S.p.A.

Macro Ambito	Responsabilità	Ruolo
Sistemi e dati «core»	Comune di Parma	Identificare e classificare i sistemi e i dati «core» necessari per garantire l'operatività
RTO e RPO	Comune di Parma	Identificare il livello accettabile di perdita dei dati e il tempo massimo necessario per recuperare i servizi «critici»
Rete dati (MPLS) Comunale	Outsourcer TLC	Garantire la connettività delle postazioni di lavoro
Rete dati (MPLS) Regionale	LEPIDA ScpA	Garantire la connettività fra i Data Center
Accesso internet	LEPIDA ScpA	Garantire la linea di pubblicazione per i servizi online
Data Center Remoto	LEPIDA ScpA	Garantire le performance minime necessarie per l'erogazione dei servizi «critici»
Gestione delle fasi operative del DRP	Comune di Parma - It.City SpA	Coordinare tutti gli attori coinvolti nel piano di disaster recovery

FASI DEL PIANO DI DISASTER RECOVERY

Le fasi riportate di seguito descrivono il processo operativo che il Comune di Parma, con il supporto di IT.CITY, deve seguire per attivare il Piano di Disaster Recovery e ripristinare la continuità dei servizi ICT in caso di disastro, indisponibilità prolungata o interruzione grave del sito primario.

Valutazione della situazione di crisi o indisponibilità del sito primario

Al verificarsi di un evento che compromette la disponibilità dei servizi ICT (guasti, incidenti infrastrutturali, eventi metereologici, indisponibilità prolungata del data center, *cyber attack*), il personale incaricato effettua una valutazione preliminare per:

- identificare la natura dell'evento (guasto locale, incidente infrastrutturale, attacco informatico, indisponibilità totale/parziale del sito);
- stimare la durata prevista dell'indisponibilità;
- verificare l'impatto sui servizi critici.

La valutazione viene immediatamente comunicata al Disaster Recovery Manager, che avvia l'analisi per determinare se sussistano le condizioni per dichiarare il disastro.

Dichiarazione del disastro

La dichiarazione formale di disastro può essere effettuata dal DR Manager, previa autorizzazione del Comitato di Crisi del Comune di Parma, quando si verificano una o più delle seguenti condizioni:

- indisponibilità del sito primario per un periodo superiore all'indisponibilità massima tollerata dai servizi critici;
- danni fisici o logici che impediscono il ripristino sul sito primario con le modalità standard;
- compromissione di sistemi essenziali che impatta la continuità dei servizi critici.

Notifica e attivazione delle strutture coinvolte

Una volta dichiarato il disastro, il DRM avvia le comunicazioni ufficiali tramite:

- Canale Teams dedicato al DRP, creato appositamente per la gestione dell'emergenza;
- eventuale supporto tramite telefono e PEC per i ruoli che richiedono formalizzazioni.

La sequenza delle notifiche prevede:

1. Allerta del Comitato di Crisi.
2. Attivazione del team di ripristino IT.CITY.
3. Comunicazione ai referenti comunali dei servizi coinvolti.
4. Allineamento costante tramite Teams, con tracciamento automatico delle comunicazioni.

Ogni notifica deve essere:

- tracciata (registro cronologico gestito dal DRM);
- confermata dal destinatario (es. via risposta nel canale Teams).

Il punto di coordinamento operativo è stabilito nel canale Teams, dove vengono condivisi aggiornamenti, documenti e evidenze di test.
Devono essere disponibili canali di comunicazione di emergenza alternativi e protetti, utilizzabili anche in caso di compromissione dell'identità digitale, della posta o di Teams; contatti e istruzioni essenziali sono mantenuti anche offline. Se il disastro deriva da un incidente potenzialmente significativo, il DRM informa immediatamente RTD e gruppo incident response e attiva la Procedura di Gestione degli Incidenti per le notifiche ACN/CSIRT Italia entro le tempistiche applicabili, preservando evidenze e cronologia delle decisioni.

Attivazione del Piano di DR e delle procedure ad esso connesse

Dopo l'attivazione formale del DRP, il DRM convoca il team tecnico e assegna eventuali ruoli straordinari non previsti dal piano (ad esempio funzioni di supplenza).
Le attività previste includono:

- verifica delle competenze necessarie rispetto alla tipologia di incidente;
- revisione del processo di ripristino e della sequenza delle azioni previste dal DRP;
- verifica della disponibilità fisica del personale nelle ore successive all'evento;
- definizione delle turnazioni;
- raccolta e analisi delle segnalazioni tecniche in arrivo dal Comune o dai servizi impattati;
- valutazione della praticabilità del ripristino in funzione del numero di risorse disponibili.

Attivazione del sito remoto di DR e avvio delle operazioni di ripristino

In caso di evento che renda necessaria l'attivazione del sito di Disaster Recovery remoto, le attività di avvio e messa in esercizio del sito secondario sono in capo a Lepida S.c.p.A., quale soggetto gestore dell'infrastruttura e del servizio di connettività.

L'attivazione del sito di DR avviene a seguito della comunicazione formale del Comune di Parma a Lepida, che provvede alle operazioni tecniche necessarie per garantire la disponibilità delle risorse elaborative, la potenza computazionale e la connettività di rete presso il data center remoto di Ferrara.

Non è previsto alcun accesso fisico da parte del personale comunale o di altri soggetti incaricati: i data center Lepida sono progettati per funzionare in modalità *unattended,* consentendo la gestione e il controllo da remoto delle infrastrutture e dei sistemi. Tutte le operazioni di accensione, configurazione e messa in esercizio del sito secondario vengono pertanto effettuate da Lepida in autonomia, nel rispetto delle procedure operative e dei livelli di servizio concordati con il Comune.

Il team di Disaster Recovery del Comune di Parma è responsabile del coordinamento complessivo e della comunicazione con Lepida, verificando l'avanzamento delle attività e la successiva riattivazione dei servizi applicativi secondo le priorità definite dal Piano.

Al termine delle attività di attivazione, Lepida comunica al Comune di Parma l'avvenuta disponibilità del sito remoto, consentendo di procedere alle fasi successive di verifica funzionale, validazione dei servizi e ripristino dell'operatività.

Ripristino dei sistemi presso il sito di DR

L'infrastruttura del sito remoto di Disaster Recovery gestita da Lepida è dimensionata per sostenere la replica dei servizi e dei dati dell'ambiente di produzione del Comune di Parma. Tale infrastruttura garantisce la disponibilità delle risorse necessarie al mantenimento delle copie aggiornate dei sistemi critici, che possono essere riassunti nelle seguenti componenti principali:

- Ambiente virtuale: intera produzione virtualizzata;
- Database Oracle RAC;
- Database cluster Microsoft SQL;
- Documenti non strutturati.

Durante tutte le operazioni di replica e ripristino, sono garantiti la riservatezza e l'integrità dei dati tramite connessioni cifrate, autenticazione a più fattori e registrazione dei log di accesso, in conformità al Regolamento (UE) 2016/679, art. 32.
Durante il ripristino devono rimanere attivi controlli minimi di sicurezza: accessi privilegiati nominativi e temporanei, MFA ove tecnicamente possibile, segregazione delle funzioni, registrazione e protezione dei log, sincronizzazione temporale, monitoraggio delle attività anomale e conservazione delle evidenze. Nei casi cyber, il recupero avviene in ambiente considerato affidabile, da immagini e copie verificate, con rotazione delle credenziali compromesse e controllo delle vulnerabilità prima della riapertura dei servizi.

Ripristino delle funzionalità di rete

Una volta attivato il sito remoto e verificata la praticabilità logica dell'infrastruttura, Lepida provvede al ripristino delle funzionalità di networking, necessarie per ristabilire la corretta comunicazione tra i sistemi e consentire la progressiva riattivazione dei servizi.
Le attività di rete comprendono la riattivazione e la verifica della connettività (VPN, VLAN, firewall, routing), nonché il controllo della disponibilità delle connessioni WAN/LAN e

dell'accessibilità ai servizi principali. Nel caso in cui la rete primaria non risulti disponibile, vengono predisposte configurazioni temporanee di rete atte a garantire la continuità dei collegamenti essenziali.
Al termine delle operazioni, Lepida documenta l'esito del ripristino e comunica al team di Disaster Recovery del Comune di Parma la disponibilità delle infrastrutture, segnalando eventuali limitazioni operative o restrizioni temporanee. Il team DR del Comune verifica quindi la corretta riattivazione dei servizi applicativi e procede con le successive fasi di validazione e test.

Verifica della praticabilità logica

A seguito del ripristino della rete, si procede all'analisi della praticabilità logica dell'infrastruttura. Il personale tecnico effettua le verifiche necessarie per confermare:

- la raggiungibilità dei sistemi virtuali;
- la disponibilità dei volumi di storage;
- l'accesso ai servizi di autenticazione;
- la corretta visibilità logica tra i sistemi primari e secondari.

I criteri di accettazione del ripristino comprendono almeno: integrità e completezza dei dati, verifica delle configurazioni e dei controlli di sicurezza, disponibilità del logging e del monitoraggio, test delle funzioni essenziali, validazione da parte del referente funzionale.
Nessun servizio è dichiarato pienamente ripristinato finché le verifiche previste non sono completate o le limitazioni residue non sono formalmente accettate.
Eventuali errori di configurazione o incoerenze logiche riscontrati durante la verifica devono essere documentati e comunicati tempestivamente al Disaster Recovery Manager (DRM) per le azioni correttive.

Verifica della funzionalità dei principali applicativi

Una volta completate le verifiche infrastrutturali, il personale tecnico applicativo, in collaborazione con il DRM, procede alla validazione dei principali sistemi software critici. Questa fase prevede:

- la ricognizione degli applicativi considerati critici ai fini della continuità operativa;
- l'esecuzione di test di base per accertare il corretto funzionamento dei sistemi;
- la registrazione degli esiti dei test nel registro delle operazioni di DR;
- la corretta visibilità logica tra i sistemi primari e secondari.

In tabella si riportano le tempistiche rilevate per le fasi del piano di DR (calcolate durante i test), ponendo attenzione ai tempi di RTO e di RPO.

Ripristino sistemi sito remoto	RTO	RPO	Attività
configurazione networking	n.a.	n.a.	Lepida
ripristino accessibilità dati non strutturati	Lepida (15 min)	Lepida (15 min)	Lepida
attivazione e configurazione Database Microsoft "replica"	30 min/db	Real time	Itcity
attivazione e configurazione Database Oracle "replica"	30 min/db	Real time	Itcity
Attivazione macchine virtuali "replica"	5 min/vm	1 ora	Itcity
Configurazione macchine virtuali "replica"	5 min/vm	None	Itcity

Configurazione e verifica Ambiente applicativo	60 min	None	Itcity
installazione hardware supplementare	n.a.	n.a.	Accordi Comune – Lepida
configurazione hardware	n.a.	n.a.	Lepida

Comunicazione relativa al completamento del processo di ripristino

Al termine delle attività di ripristino, DRM formalizza la chiusura delle operazioni attraverso:

1) comunicazione nel canale Teams dedicato al DRP;
2) comunicazione telefonica e posta elettronica certificata per i ruoli che richiedono formalizzazione.

La comunicazione deve contenere:

- elenco dei servizi ripristinati;
- tempi effettivi di ripristino;
- eventuali limitazioni residue;
- data e ora di rientro in operatività.

Inoltre, il DRM deve conservare la comunicazione nel registro degli eventi e aggiornare il piano di Disaster Recovery qualora durante le operazioni siano emerse criticità.

Ripristino del sito primario e "Dichiarazione di fine emergenza"

Una volta concluso con esito positivo il ripristino dei servizi presso il sito di Disaster Recovery, il Disaster Recovery Manager valuta la disponibilità del sito primario e le condizioni per il rientro alla normale operatività.

Le attività principali prevedono:

- il ripristino delle connessioni di rete e la verifica della piena connettività tra i siti;
- la replica dei dati e dei backup dal sito di Disaster Recovery verso il sito primario, per riallineare le informazioni aggiornate durante la fase di emergenza;
- lo switch progressivo delle macchine virtuali e dei database sul sito primario, fino al completo ritorno all'operatività ordinaria.

Durante questa fase, viene assicurato che i dati e i servizi ripristinati nel sito di DR siano allineati con quelli del sito primario, al fine di evitare perdita di informazioni o incoerenze tra gli ambienti.

Completato il ripristino dell'ambiente primario, il DRM procede alla "Dichiarazione di fine emergenza", che sancisce la chiusura formale del Piano di Disaster Recovery e il ritorno allo stato di normalità operativa. La dichiarazione deve essere comunicata attraverso i canali ufficiali (Teams) e deve contenere almeno:

- la conferma dell'avvenuto ripristino dell'operatività primaria;
- la data e l'ora di chiusura dell'emergenza;
- l'indicazione delle eventuali attività residue o azioni di follow-up;
- la segnalazione di eventuali aggiornamenti da apportare al Piano o alle procedure operative.

Successivamente, il DRM provvede ad aggiornare il registro degli eventi di DR e ad avviare, se necessario, un'attività di analisi post-evento, finalizzata a valutare l'efficacia delle procedure adottate, i tempi effettivi di risposta e gli eventuali miglioramenti da introdurre nel Piano di Disaster Recovery.

Analisi post-evento e miglioramento continuo

Dopo la dichiarazione di fine emergenza, il Disaster Recovery Manager coordina una revisione post-evento finalizzata a valutare l'efficacia complessiva delle attività di ripristino e a individuare eventuali criticità riscontrate durante la gestione dell'emergenza.
L'analisi post-evento ha l'obiettivo di:

- verificare la coerenza tra le procedure adottate e le previsioni del Piano di Disaster Recovery;
- identificare le lezioni apprese e le opportunità di miglioramento;
- proporre eventuali azioni correttive o aggiornamenti delle procedure operative;
- aggiornare, se necessario, la documentazione tecnica, i contatti di emergenza e le tempistiche di ripristino.

Al termine della revisione, il DRM redige un rapporto di analisi post-evento, che viene condiviso con il Comitato di Crisi per approvazione. Il rapporto costituisce base per l'aggiornamento periodico del Piano di Disaster Recovery e per il miglioramento continuo del processo di gestione delle emergenze.

TEST DELL'INFRASTRUTTURA E DEL PIANO

Il presente capitolo definisce le modalità di verifica e validazione del Piano di Disaster Recovery, con l'obiettivo di garantire che le procedure operative, le infrastrutture e i tempi di ripristino siano coerenti con quanto pianificato. I test periodici consentono di valutare l'efficacia complessiva del Piano, individuare eventuali criticità e introdurre azioni di miglioramento continuo.

SPECIFICA DELLA METODOLOGIA ADOTTATA

Le attività di test del Piano si articolano in due tipologie principali, da eseguire con periodicità differenziata:

- Test tecnico di simulazione operativa (*simulation test*): da effettuarsi ogni sei mesi, consiste nell'avvio controllato di un gruppo selezionato di macchine virtuali presenti nel sito di Disaster Recovery, comprensivo dell'accensione e dello spegnimento coordinato dei sistemi, inclusi i database (Oracle e Microsoft SQL). Le simulazioni vengono eseguite a rotazione su insiemi diversi di macchine, al fine di verificare la capacità effettiva di ripristino delle componenti infrastrutturali e applicative.
- Esercitazione di tipo *"table-top"* (*table-top exercise*): da effettuarsi una volta all'anno, consiste in una simulazione teorica in cui il team di Disaster Recovery, riunito in modalità remota su Teams, dichiara l'attivazione del piano e discute in tempo reale le azioni da intraprendere in base allo scenario ipotizzato. Questo test ha lo scopo di verificare la prontezza organizzativa, la chiarezza dei ruoli e la correttezza dei flussi di comunicazione tra le diverse figure coinvolte.

SPECIFICHE RELATIVE ALLA INDIVIDUAZIONE DELLA FINESTRA TEMPORALE

Le prove tecniche sull'infrastruttura vengono pianificate con cadenza semestrale, preferibilmente in fasce orarie di basso impatto operativo, al fine di non compromettere la continuità dei servizi in esercizio. Le esercitazioni *table-top* vengono invece programmate una volta all'anno. Ogni test deve essere preceduto da una comunicazione formale indirizzata ai soggetti coinvolti, con indicazione della data, dell'orario e degli obiettivi specifici della simulazione.

PIANIFICAZIONE DEL TEST

La pianificazione dei test è di competenza del Disaster Recovery Manager, il quale definisce:

- l'ambito e le componenti oggetto della simulazione;
- la finestra temporale;
- il personale coinvolto e le responsabilità operative.

L'esecuzione dei test è a cura del personale tecnico, sotto la supervisione del DRM, che monitora le attività e raccoglie gli esiti. Al termine di ogni esercitazione, deve essere compilato un verbale di test, che documenti:

- la data e l'ora di avvio e conclusione;
- i sistemi e le componenti coinvolte;
- le operazioni effettuate;
- gli esiti e le eventuali anomalie riscontrate;
- le azioni correttive da intraprendere.

Il verbale di test deve essere conservato nel registro ufficiale delle prove di DR del Comune di Parma. Tale documentazione costituisce evidenza ai fini di eventuali attività di audit o verifiche di conformità.

Il programma di test deve includere, secondo il rischio, ripristino da backup offline o immutabile, indisponibilità delle credenziali o dei canali ordinari, simulazione compromissione ransomware, simulazione guasto dei servizi cloud o dei fornitori, perdita della connettività e rientro controllato al sito primario. Per ogni prova sono rilevati RTO/RPO effettivi, integrità dei dati, efficacia dei controlli, tempi dei fornitori e capacità dei responsabili di assumere decisioni. Gli esiti negativi generano azioni correttive con responsabile e scadenza e aggiornano Registro dei Rischi, SoA e Piano di Trattamento/Adeguamento.

DEBRIEFING E RAPPORTO FINALE DI TEST

Al termine di ciascun test, il DRM convoca una sessione di debriefing per l'analisi dei risultati. Durante la riunione vengono discussi:

- gli esiti della simulazione;
- le criticità riscontrate;
- le azioni correttive o migliorative da adottare;
- le eventuali modifiche da apportare al Piano di Disaster Recovery.

A conclusione del debriefing, viene redatto un rapporto finale di test, firmato dal DRM, che riassume i risultati e le decisioni assunte. Il rapporto deve essere conservato unitamente ai verbali di test e costituirà riferimento per le successive revisioni del Piano e per gli audit periodici.

MANUTENZIONE DEL PIANO DI DISASTER RECOVERY

La manutenzione del Piano di Disaster Recovery è un processo continuo finalizzato a garantirne l'efficacia nel tempo e la coerenza con l'evoluzione tecnologica, organizzativa e procedurale del Comune. Il Piano deve essere aggiornato ogniqualvolta si verifichino modifiche che possano influire sulle modalità di risposta o di ripristino dei servizi critici.

EVENTI CHE PREVEDONO IL RIESAME

Il Piano deve essere riesaminato con cadenza almeno annuale o ogniqualvolta si verifichino eventi che possano influire sulle modalità di gestione della continuità operativa e del ripristino dei sistemi.
In particolare, il riesame deve essere effettuato a seguito di:

- esecuzione di test o simulazioni di disaster recovery, per recepire eventuali criticità emerse;
- incidenti reali che abbiano comportato l'attivazione del piano, anche parziale;
- modifiche infrastrutturali significative (introduzione di nuovi sistemi, server o ambienti virtuali);
- aggiornamenti contrattuali o variazioni dei fornitori ICT che gestiscono componenti critiche;
- variazioni organizzative che comportano cambi di ruoli, responsabilità o recapiti di riferimento.

Ogni revisione deve essere formalmente approvata e registrata nel Registro delle revisioni del Piano.

In occasione del riesame il DRM e il RTD verificano la coerenza del DRP con BIA, inventario degli asset, architetture, contratti, classificazione delle informazioni, Piano di Business Continuity, Piano di Gestione delle Crisi, Procedura Incidenti e Dichiarazione di Applicabilità. Il riesame considera anche l'efficacia dei controlli A.5.23, A.5.30, A.8.9 e A.8.16 e documenta eventuali rischi residui o non conformità.

PROCESSO DI CHANGE

Il processo di *change* definisce le modalità con cui viene gestito l'aggiornamento del Piano di Disaster Recovery, dalla segnalazione dell'evento che lo richiede fino al rilascio della nuova versione approvata.
Tale processo si articola nelle seguenti fasi principali:

1. Segnalazione dell'evento o richiesta di *change*;
2. Verifica e valutazione degli impatti;
3. Esecuzione, validazione e chiusura del *change*.

Ogni *change* deve essere tracciato mediante un registro delle revisioni e una tabella di tracciabilità, riportante almeno:

- ID del *change*;
- data di apertura e chiusura;
- descrizione sintetica della modifica;
- autore e referenti coinvolti;
- livello di *change* (minore, maggiore, urgente);
- impatti sui servizi, sui sistemi e sulla documentazione;
- approvazioni e versione rilasciata.

I trigger che possono determinare l'attivazione del processo di *change* includono:

- introduzione di nuovi sistemi, tecnologie o fornitori;
- modifiche all'infrastruttura IT o alle modalità di erogazione dei servizi;
- risultati di test o incidenti reali;

- variazioni organizzative, di personale o di responsabilità;
- aggiornamenti normativi o regolamentari.

I livelli di *change* sono così definiti:

- *change* minore: aggiornamento di dettaglio che non modifica il contenuto operativo del Piano (es. aggiornamento contatti, revisioni formali);
- *change* maggiore: modifica sostanziale che impatta su procedure, ruoli o architetture tecnologiche, e richiede una nuova versione del Piano;
- *change* urgente: modifica da applicare con priorità immediata per garantire la continuità operativa o correggere errori critici.

Tutti i *change* devono essere formalmente approvati dal Responsabile IT.CITY/DRM e dal referente comunale prima della distribuzione della nuova versione del documento.

Segnalazione evento

Possono proporre una modifica del Piano:

- il Disaster Recovery Manager;
- i responsabili di area o di servizio;
- i referenti applicativi;
- i fornitori esterni coinvolti nella gestione operativa o infrastrutturale.

La segnalazione deve essere formalizzata mediante un modulo di richiesta *change*, contenente almeno:

- ID richiesta e data di presentazione;
- nome e ruolo del richiedente;
- motivazione o trigger del *change*;
- ambito interessato (tecnologico, procedurale, organizzativo);
- livello di urgenza;
- eventuali documenti o evidenze a supporto.

La richiesta viene registrata nel registro *change* e trasmessa al DRM per l'avvio delle successive valutazioni.

Verifica impatti

Il DRM, in coordinamento con i referenti tecnici e organizzativi, valuta:

- gli impatti del *change* sui servizi critici e sulle procedure operative;
- i rischi, i costi e i tempi di implementazione;
- le dipendenze da altri sistemi o processi;
- la necessità di effettuare test, aggiornamenti formativi o comunicazioni interne.

Sulla base della valutazione, viene predisposto un piano di implementazione e, ove necessario, un piano di reversibilità per garantire il ripristino della versione precedente del DRP in caso di criticità.

Esecuzione change

L'esecuzione del *change* deve essere pianificata in dettaglio, definendo:

- i responsabili delle attività;
- la finestra operativa per l'applicazione delle modifiche;
- le comunicazioni ai soggetti coinvolti;
- l'eventuale test *post-change* per verificarne l'efficacia.

Successivamente, devono essere aggiornati:

- il documento del DRP e i relativi allegati (liste contatti, priorità servizi, procedure operative, topologie di rete, ecc.);
- il numero di versione e il *changelog*;
- la tabella di tracciabilità delle revisioni.

Il DRM provvede a validare il *change*, raccogliere le evidenze (es. verbali di test, approvazioni) e distribuire il documento aggiornato ai destinatari autorizzati. Infine, *il change* viene chiuso nel registro indicando la data di chiusura, l'esito e eventuali azioni correttive residue.

FORMAZIONE

Al fine di garantire l'efficace attuazione e il corretto mantenimento del Piano di Disaster Recovery e delle attività di gestione della crisi, l'Ente coordinerà un programma di formazione e sensibilizzazione rivolto al personale coinvolto nei processi di Disaster Recovery e, progressivamente, all'intera popolazione aziendale.
Le attività di awareness includeranno comunicazioni interne, la pubblicazione della documentazione sulla intranet istituzionale e momenti formativi dedicati ai Responsabili di Settore e al personale dei servizi essenziali.
La formazione sarà finalizzata a illustrare i principali contenuti, ruoli e responsabilità previsti dal Disaster Recovery Plan.

ALLEGATI

SCHEDE DI BUSINESS IMPACT ANALYSIS
BUSINESS CONTINUITY PLAN
ORGANIZZAZIONE PER LA SICUREZZA INFORMATICA - RUOLI E RESPONSABILITA' PER LA GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI