Comune di Parma

Piano di Gestione delle Crisi

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: 26/01/2026
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. Il documento è accessibili all'interno di un repository

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. La presente procedura, 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

1. INTRODUZIONE 5
2. SCOPO E CAMPO DI APPLICAZIONE 5
3. RIFERIMENTI NORMATIVI E DOCUMENTALI 6
4. RELAZIONE CON GLI ALTRI PIANI 6
4.1 GESTIONE INCIDENTI 6
4.2 BUSINESS CONTINUITY 7
4.3 DISASTER RECOVERY 7
4.4 SISTEMA DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI 7
5. CRITERI DI ATTIVAZIONE DELLA CRISI 7
6. COMITATO DI CRISI 8
7. FASI DI GESTIONE DELLA CRISI 8
FASE 1 – VALUTAZIONE 8
FASE 2 – COORDINAMENTO 9
FASE 3 – GESTIONE DELLA CONTINUITÀ OPERATIVA 9
FASE 4 – RIPRISTINO 9
FASE 5 – RIENTRO ALLA NORMALITÀ 10
8. COMUNICAZIONI DI CRISI 10
9. CHIUSURA E MIGLIORAMENTO 10
APPENDICE A – MATRICE DI ATTIVAZIONE DEI PIANI 12
A.1 Livelli di escalation *12*
A.2 Esempi di applicazione *12*
A.4 Ruoli coinvolti per livello *13*
A.5 Criteri per la chiusura della crisi *13*

1. INTRODUZIONE

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 risponde ai requisiti di continuità operativa, disaster recovery e gestione delle crisi previsti dalla misura ID.IM-04 dell'Allegato 1 alla Determinazione ACN n. 164179 del 14 aprile 2025.

Il presente Piano costituisce parte integrante del framework documentale adottato dal Comune di Parma per il governo della sicurezza delle informazioni e della cybersicurezza. Per gli aspetti operativi relativi ai sistemi e ai servizi affidati, il Piano si raccorda con il Sistema di Gestione per la Sicurezza delle Informazioni (SGSI) di IT.CITY S.p.A. e con le relative politiche, procedure e misure di sicurezza, per quanto applicabili.

Il Piano si inserisce nel sistema documentale del Comune di Parma e si raccorda, in particolare, con la Procedura di Gestione degli Incidenti di Sicurezza delle Informazioni, la Valutazione dei rischi, il Piano di Trattamento del rischio, il Piano di Adeguamento, il Piano di Business Continuity e il Piano di Disaster Recovery. Il relativo modello di gestione è definito in coerenza con i principi di governo, pianificazione, supporto, attività operative, valutazione delle prestazioni e miglioramento continuo applicabili nell'ambito del sistema di gestione della sicurezza delle informazioni.

2. SCOPO E CAMPO DI APPLICAZIONE

Il presente Piano definisce le modalità organizzative e decisionali adottate dal Comune di Parma per la gestione delle situazioni di crisi derivanti da incidenti di sicurezza delle informazioni, eventi di indisponibilità dei sistemi informativi o altri eventi che possano compromettere la continuità dei servizi istituzionali.

Il Piano costituisce il livello di coordinamento strategico tra:

- Procedura di Gestione degli Incidenti di Sicurezza delle Informazioni;
- Piano di Business Continuity;
- Piano di Disaster Recovery;
- Sistema di Gestione per la Sicurezza delle Informazioni (SGSI).

La finalità del Piano è garantire una gestione coordinata delle situazioni di emergenza assicurando:

- tutela delle informazioni;
- continuità dei servizi essenziali;
- riduzione degli impatti sull'Ente;
- rispetto degli obblighi normativi;
- tempestivo ritorno alla normale operatività.

Il Piano si applica a tutte le situazioni nelle quali un incidente di sicurezza:

- provoca o può provocare indisponibilità significativa dei servizi ICT;
- compromette informazioni o sistemi critici;
- richiede l'attivazione di misure straordinarie di continuità operativa;
- richiede il coinvolgimento della Direzione dell'Ente;
- comporta obblighi di notifica verso ACN, CSIRT Italia, Garante Privacy o altre Autorità competenti.

Il Piano è sottoposto a verifica periodica mediante esercitazioni o simulazioni coordinate con la Procedura di Gestione degli Incidenti, il Piano di Business Continuity e il Piano di Disaster Recovery.

3. RIFERIMENTI NORMATIVI E DOCUMENTALI

- Codice dell'Amministrazione Digitale (CAD)
- Serie di standard ISO/IEC 27000:2018 - Sicurezza e Gestione delle Informazioni
- Standard ISO/IEC 27001:2022 - Sistema di Gestione della Sicurezza delle Informazioni (SGSI)
- Standard ISO/IEC 27002:2022 - Controlli di sicurezza delle informazioni e cybersecurity
- Standard ISO/IEC 27005:2022 - Gestione dei rischi di sicurezza delle informazioni
- D.Lgs. 196/2003 - codice in materia di protezione dei dati personali aggiornato con D.Lgs. 101/2018 per adeguamento al Regolamento Europeo 679/2016 (GDPR)
- D.Lgs. 138/2024 - recepimento della Direttiva (UE) 2022/2555 NIS2
- Provvedimenti e Autorizzazioni Generali dell'Autorità Garante e qualsiasi altra norma applicabile avente ad oggetto il trattamento di dati personali
- Contratto di Servizio per la gestione del sistema informativo tra Comune di Parma ed IT City SPA.
- Determinazione del Direttore generale dell'ACN (Agenzia per la Cybersicurezza Nazionale) n. 164179 del 14 aprile 2025 – Allegato 1 "Misure di sicurezza di base per i soggetti importanti"
- Framework documentale specifico Comune di Parma
- Framework documentale IT.CITY S.P.A. Sistema di Gestione della Sicurezza delle Informazioni (SGSI)

4. RELAZIONE CON GLI ALTRI PIANI

4.1 Gestione Incidenti

La Procedura di Gestione degli Incidenti rappresenta il primo livello di risposta operativa.

Essa disciplina:

- rilevazione;
- registrazione;
- analisi;

- contenimento;
- trattamento degli incidenti.

Qualora l'evento superi le normali capacità di gestione operativa o presenti impatti significativi, viene attivato il presente Piano di Gestione delle Crisi.

4.2Business Continuity

Qualora la crisi comporti l'interruzione o il grave degrado dei servizi essenziali, il Comitato di Crisi può disporre l'attivazione del Piano di Business Continuity.

Le misure di continuità operativa hanno l'obiettivo di garantire il mantenimento delle funzioni critiche dell'Ente durante la gestione della crisi.

4.3Disaster Recovery

Nel caso in cui l'evento coinvolga infrastrutture o sistemi informatici critici, il Comitato di Crisi può autorizzare l'attivazione del Piano di Disaster Recovery.

Le attività di Disaster Recovery sono finalizzate al ripristino controllato di:

- infrastrutture;
- sistemi;
- basi dati;
- servizi informatici.

4.4Sistema di Gestione per la Sicurezza delle Informazioni

Il Pianocontribuisce al conseguimento degli obiettivi di:

- disponibilità;
- integrità;
- riservatezza;
- autenticità delle informazioni.

Le evidenze derivanti dalla gestione delle crisi costituiscono input per il miglioramento continuo La Procedura Incidenti resta il riferimento per rilevazione, classificazione, gestione tecnica e notifiche; il presente Piano disciplina il coordinamento strategico e decisionale. L'attivazione di BC o DR non sospende le attività di contenimento, analisi forense, conservazione delle evidenze o comunicazione alle Autorità. Le decisioni di attivazione, sospensione e chiusura dei piani sono registrate in un unico diario di crisi.

5. CRITERI DI ATTIVAZIONE DELLA CRISI

Una situazione di crisi viene dichiarata quando si verifica almeno una delle seguenti condizioni:

- indisponibilità prolungata di servizi essenziali;
- compromissione di sistemi critici;
- attacco ransomware esteso;
- esfiltrazione massiva di dati;

- impossibilità di garantire i livelli minimi di servizio;
- impatto significativo sulla reputazione dell'Ente;
- necessità di assumere decisioni strategiche urgenti.

Ai fini del presente Piano, il Comune di Parma adotta una scala interna di escalation articolata su quattro livelli (L1-L4), finalizzata a determinare il progressivo coinvolgimento delle strutture organizzative competenti e, ove necessario, l'attivazione del Piano di Gestione delle Crisi, del Piano di Business Continuity e del Piano di Disaster Recovery.

La classificazione secondo i livelli L1-L4 ha finalità esclusivamente organizzative e non sostituisce i criteri previsti dalla normativa applicabile per la qualificazione degli incidenti.

6. COMITATO DI CRISI

Il comitato di Crisi è il gruppo di direzione e coordinamento attivato in presenza di incidenti di sicurezza, eventi di indisponibilità dei servizi ICT o situazioni che possano compromettere la continuità operativa dell'Ente.

Ha il compito di assumere le decisioni strategiche, coordinare le strutture coinvolte, autorizzare le comunicazioni verso l'esterno, supervisionare le attività di risposta e ripristino e garantire il ritorno alla normale operatività.

Il Comitato di Crisi è composto dalle seguenti figure di riferimento:

- Sindaco o Assessore delegato alla Transizione Digitale
- Direttore Generale / Segretario Generale
- Dirigente Responsabile per la Transizione Digitale / CIO
- Responsabile della Comunicazione Istituzionale

In funzione della tipologia di evento, il Comitato di Crisi può avvalersi delle seguenti figure di riferimento:

- Amministratore Unico/Direttore Operativo IT.CITY S.p.A.
- Data Protection Officer (DPO)
- Responsabile Protezione Civile
- Responsabili dei servizi comunali impattati

Il Comitato di Crisi opera sulla base delle informazioni, delle valutazioni tecniche e delle proposte formulate dal Gruppo di Coordinamento e Gestione degli Incidenti di Sicurezza, che assicura il supporto operativo necessario per la gestione degli eventi e delle situazioni di crisi.
Gli Organi di Amministrazione e Direttivi approvano le modalità di implementazione del Piano e ne sovrintendono l'efficacia. Il RTD assicura il raccordo con modello organizzativo e di governo per la gestione della sicurezza delle informazioni e della cybersicurezza ACN e strutture tecniche; il Comitato assume le decisioni strategiche; IT.CITY e i fornitori attuano le attività operative secondo gli accordi vigenti.

7. FASI DI GESTIONE DELLA CRISI

Fase 1 – Valutazione

Il Comitato:

- riceve le informazioni dal gruppo di gestione degli incidenti;

- valuta impatti e scenari;
- determina il livello di severità.

La valutazione iniziale comprende servizi e cittadini impattati, durata prevedibile, dipendenze e fornitori coinvolti, rischio per dati personali e informazioni classificate, possibile impatto transfrontaliero, indicatori di compromissione disponibili, necessità di preservare evidenze e sussistenza dei criteri di incidente significativo. Il fornitore coinvolto deve trasmettere senza ritardo le informazioni necessarie alla valutazione e alle notifiche del Comune.

Fase 2 – Coordinamento

Il Comitato:

- assegna le priorità;
- coordina i soggetti coinvolti;
- autorizza le comunicazioni;
- valuta l'attivazione di BC e DR.

A seguito dell'attivazione del Piano è istituito un diario di crisi, che costituisce il riferimento documentale unitario per la registrazione degli eventi rilevanti, delle decisioni assunte, dei soggetti coinvolti, delle azioni disposte, delle comunicazioni effettuate, delle tempistiche e delle evidenze prodotte.

Fase 3 – Gestione della Continuità Operativa

Qualora necessario:

- viene attivato il Piano di Business Continuity;
- vengono adottate modalità operative alternative;
- vengono individuati i processi prioritari da garantire.

Le priorità e i livelli minimi di servizio sono quelli approvati nella BIA e nel Piano di Business Continuity. Ogni deroga o limitazione temporanea deve essere valutata rispetto a sicurezza, obblighi di legge e impatto sui cittadini, approvata dal ruolo competente e registrata con durata, motivazione e misure compensative.

Fase 4 – Ripristino

Qualora necessario:

- viene attivato il Piano di Disaster Recovery;
- vengono eseguite le attività di recupero;
- viene verificata l'integrità dei sistemi ripristinati.

Nei casi di compromissione cyber, il ripristino deve avvenire da copie e configurazioni verificate, in ambiente considerato affidabile, con controllo degli accessi privilegiati, rotazione delle credenziali, logging e monitoraggio attivi, verifica delle vulnerabilità e validazione dei referenti di servizio prima della riapertura completa.

Fase 5 – Rientro alla Normalità

Il Comitato:

- verifica il ripristino dei servizi;
- valuta il rischio residuo;
- dichiara conclusa la crisi.

8. COMUNICAZIONI DI CRISI

Le comunicazioni devono essere:

- tempestive;
- coordinate;
- coerenti;
- autorizzate dal Comitato di Crisi.

La comunicazione può coinvolgere:

- personale;
- cittadini;
- fornitori;
- ACN;
- CSIRT Italia;
- Garante Privacy;
- altri soggetti istituzionali.

Gli obblighi di notifica relativi agli incidenti significativi sono gestiti secondo quanto disciplinato dalla Procedura di Gestione degli Incidenti di Sicurezza delle Informazioni e dalla normativa applicabile. Il Comitato di Crisi assicura il necessario coordinamento tra le notifiche regolamentari e le comunicazioni istituzionali rivolte al personale, ai cittadini, ai fornitori e agli altri soggetti interessati.

9. CHIUSURA E MIGLIORAMENTO

Al termine della crisi è redatto un Rapporto Finale contenente:

- descrizione dell'evento;
- cronologia degli interventi;
- impatti registrati;
- efficacia delle misure adottate;
- criticità rilevate;
- azioni correttive;
- opportunità di miglioramento.

Il Rapporto costituisce informazione documentata ed è utilizzato nell'ambito del Riesame della Direzione e del miglioramento continuo del sistema.

Il rapporto di chiusura deve includere anche la valutazione della significatività NIS2, le notifiche effettuate, i tempi effettivi di risposta e ripristino, le decisioni del Comitato, le prestazioni dei fornitori, il rischio residuo e le evidenze conservate. Le azioni correttive sono assegnate con responsabile e scadenza e comportano, ove necessario, aggiornamento della Valutazione del rischio, BIA, BC, DR, Procedura Incidenti, contratti e Piano di Trattamento/Adeguamento.

Il Piano è sottoposto periodicamente a esercitazioni e simulazioni, sulla base della programmazione definita dall'Ente e ogniqualvolta variazioni significative del contesto, dei servizi, dell'organizzazione o delle infrastrutture rendano opportuno verificarne l'efficacia.

APPENDICE A – MATRICE DI ATTIVAZIONE DEI PIANI

La presente matrice definisce i criteri di attivazione coordinata della Procedura di Gestione degli Incidenti, del Piano di Gestione delle Crisi, del Piano di Business Continuity e del Piano di Disaster Recovery.

L'obiettivo è garantire una gestione proporzionata all'impatto dell'evento, evitando sia sottovalutazioni sia attivazioni non necessarie delle strutture di crisi

A.1 Livelli di escalation

Livello	Scenario	Gestione Incidenti	Comitato di Crisi	Business Continuity	Disaster Recovery
L1	Evento limitato senza impatto sui servizi	SI	NO	NO	NO
L2	Evento significativo con impatto contenuto su uno o più servizi	SI	Valutazione RTD	NO	NO
L3	Interruzione di servizi critici o rischio elevato per l'Ente	SI	SI	SI	Valutazione
L4	Grave compromissione dei sistemi o indisponibilità prolungata	SI	SI	SI	SI

A.2 Esempi di applicazione

Scenario	Livello	Azioni previste
Malware su singola postazione senza propagazione	L1	Gestione tecnica dell'incidente
Compromissione account con accesso non autorizzato a dati	L2	Gestione incidente e valutazione impatti
Attacco ransomware su più uffici con indisponibilità dei servizi	L3	Attivazione Comitato di Crisi e Business Continuity
Indisponibilità del Data Center primario	L4	Attivazione Comitato di Crisi, Business Continuity e Disaster Recovery
Indisponibilità del protocollo informatico per diverse ore	L3	Attivazione Business Continuity e valutazione DR
Esfiltrazione massiva di dati personali	L3	Attivazione Comitato di Crisi e gestione obblighi normativi
Compromissione completa dell'infrastruttura ICT comunale	L4	Attivazione completa dei piani

A.3 Ruoli coinvolti per livello

Ruolo	L1	L2	L3	L4
Gruppo Sicurezza / Incident Response	X	X	X	X
RTD	Informato	Coinvolto	X	X
DPO	Se necessario	Se necessario	X	X
Direttore Generale / Segretario Generale	-	Informato	X	X
Sindaco / Giunta	-	Informato	X	X
Responsabile Comunicazione	-	-	X	X
Comitato di Crisi	-	Valutazione	X	X

A.4 Criteri per la chiusura della crisi

La crisi può essere dichiarata conclusa quando risultano contemporaneamente soddisfatte le seguenti condizioni:

- l'incidente è stato contenuto e trattato;
- i sistemi e i servizi essenziali sono stati ripristinati;
- le attività di Disaster Recovery sono state concluse (se attivate);
- i livelli di servizio risultano stabilizzati;
- sono state effettuate le notifiche previste dalla normativa applicabile;
- il Comitato di Crisi approva formalmente il ritorno alla normale operatività;
- viene avviata la fase di analisi post-evento e miglioramento continuo