Comune di Parma

PIANO DI ADEGUAMENTO DELLA SICUREZZA INFORMATICA

Documento per approvazione formale ai fini ID.IM-01

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 5
3. RIFERIMENTI NORMATIVI E DOCUMENTALI 5
4. MATRICE DELLE AZIONI DI ADEGUAMENTO 7
5. MONITORAGGIO DEL PIANO 10
6. REPORTING AGLI ORGANI DI AMMINISTRAZIONE E DIRETTIVI 10
7. RIESAME 11

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.

A seguito degli esiti delle attività di riesame, delle verifiche di conformità, delle valutazioni del rischio e delle attività di monitoraggio della sicurezza informatica, il presente Piano individua gli interventi di adeguamento necessari a garantire l'attuazione e il miglioramento continuo delle politiche di sicurezza applicabili all'Ente.

Il Piano costituisce lo strumento attraverso il quale il Comune di Parma programma, prioritizza, monitora e documenta gli interventi necessari a colmare i gap rilevati e a migliorare progressivamente il proprio livello di sicurezza, assicurando la tracciabilità tra le carenze individuate, i rischi correlati, le misure di adeguamento e le evidenze della loro attuazione.

2. SCOPO

Il Piano persegue i seguenti obiettivi:

- rafforzare il livello di sicurezza informatica dell'Ente;
- assicurare l'attuazione delle politiche di sicurezza;
- migliorare la capacità di prevenzione, rilevazione e risposta agli incidenti;
- incrementare la resilienza operativa dei servizi digitali;
- supportare la conformità ai requisiti NIS2;
- garantire il miglioramento continuo delle misure di sicurezza.
- pianificare e monitorare la progressiva risoluzione dei gap individuati rispetto ai requisiti normativi, organizzativi e tecnici applicabili;
- assicurare la tracciabilità delle azioni di adeguamento, delle responsabilità, delle tempistiche e delle relative evidenze di attuazione.

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)

Comune di Parma

4. MATRICE DELLE AZIONI DI ADEGUAMENTO

Criteri di tracciabilità delle azioni

Ogni azione del Piano deve derivare da una o più fonti documentate: Valutazione dei rischi, audit, incidenti, vulnerabilità, modifiche normative o riesami.

Le scadenze e i budget non ancora approvati sono mantenuti con placeholder espliciti e non sono considerati impegni definitivi. Le azioni scadute o ad alta criticità sono sottoposte senza ritardo al RTD e, ove rilevanti, agli Organi di Amministrazione e Direttivi; la chiusura richiede evidenze verificabili e l'eventuale accettazione formale del rischio residuo.

Tipologia	Livello di maturità atteso (to be)	Riferimento categoria	Interventi/attività	Scadenza	Budget previsto (€)
Documenti	Implementato	Asset Management (ID.AM)	Aggiornamento Governance	2027	15.000,00 €
Documenti	Implementato	Asset Management (ID.AM)	Aggiornamento Governance	2028	15.000,00 €
Documenti	Implementato	Risk Assessment (ID.RA)	Proseguimento del progetto di BIA sui servizi core del Comune di Parma	2027	20.000,00 €
	Implementato	Risk Management Strategy (ID.RM)			
Servizio	Implementato	Supply Chain Risk Management (ID.SC)	Proseguimento della valutazione del livello di sicurezza degli applicativi gestiti da fornitori terzi tramite processi di PenTest e VA	2027	25.000,00 €
Servizio	Implementato	Awareness and Training (PR.AT)	proseguimento piano formativo di Cyber security awareness tramite piattaforma cloud CyberGuru	2027	25.000,00 €

Tipologia	Livello di maturità atteso (to be)	Riferimento categoria	Interventi/attività	Scadenza	Budget previsto (€)
Servizio	Ottimizzato	Risk Assessment (ID.RA)	potenziamento servizio SOC - proattività e threat analisys evoluta	2028	110.000,00 €
Strumenti	Implementato	Security Continuous Monitoring (DE.CM)	potenziamento servizio NGFW e sistema controllo accessi NAC	2028	50.000,00 €
Strumenti	Implementato	Protective Technology (PR.PT)	potenziamento degli strumenti di produttività individuali cloud (Microsoft 365)	2028	100.000,00 €
Strumenti	Implementato	Protective Technology (PR.PT)	potenziamento degli strumenti di produttività individual locali (Microsoft Office)	2026	40.000,00 €
Strumenti	Implementato	Protective Technology (PR.PT)	AntiDDOS	2027	15.000,00 €
Strumenti	Implementato	Protective Technology (PR.PT)	Sistema di gestione patching server	2026	20.000,00 €
Strumenti	Implementato	Protective Technology (PR.PT)	VA interno (NESSUS)	2027	20.000,00 €
Strumenti	Implementato	Protective Technology (PR.PT)	Sistema produzione copie di sicurezza (Backup)	2028	20.000,00 €
Documenti / Governance	Da pianificare	GV.OV / GV.RR / ID.IM - ISO 4-10, - NIS2 artt. 7, 23-24	Formalizzare owner e matrice RACI; collegare registro rischi, Piano; calendarizzare registrazione/aggiornamento ACN; tracciare formazione e approvazioni degli organi di vertice.	2027	N.A.

Tipologia	Livello di maturità atteso (to be)	Riferimento categoria	Interventi/attività	Scadenza	Budget previsto (€)
Processi / Monitoraggio	Da pianificare	ID.RA / DE.CM - ISO A.5.7, A.8.16 - NIS2 art. 24	Istituire processo di threat intelligence; definire fonti, responsabilità e diffusione; completare use case di logging/SIEM-SOC, soglie, retention, KPI e riesame dell'efficacia.	2027	N.A.
Tecnologie / Cloud	Da pianificare	PR.PS / GV.SC - ISO A.5.23, A.8.9 - NIS2 art. 24	Definire baseline di sicurezza cloud e configurazione; inventario e ownership; hardening, change control, configurazioni approvate, monitoraggio drift e requisiti contrattuali dei provider.	2027	N.A.
Continuità / Fisico	Da pianificare	PR.IR / RC.RP - ISO A.5.30, A.7.4 - NIS2 art. 24	Integrare BIA, BC e DR con test di prontezza ICT, RTO/RPO e dipendenze; verificare monitoraggio fisico delle aree critiche, gestione allarmi, registrazioni e prove periodiche.	2027	N.A.
Dati / Protezione	Da pianificare	PR.DS - ISO A.8.10, A.8.11, A.8.12, A.8.23 - NIS2 art. 24	Definire retention e cancellazione sicura; criteri di masking; regole DLP e gestione alert; web filtering basato sul rischio, eccezioni autorizzate, monitoraggio e metriche.	2027	N.A.
Sviluppo / Accessi / Fornitori	Da pianificare	PR.AA / PR.PS / GV.SC - ISO A.8.28 - NIS2 art. 24	Applicare secure coding e controlli SAST/DAST ove pertinenti; rafforzare clausole e notifica a cascata; estendere MFA, crittografia e comunicazioni sicure ai servizi e agli accessi a rischio.	It.city	30.000.00 €

5. MONITORAGGIO DEL PIANO

Il Responsabile per la Transizione Digitale, con il supporto di IT.CITY S.p.A., verifica periodicamente lo stato di avanzamento delle azioni previste nel presente Piano.

Per ciascun intervento sono registrati:

- percentuale di completamento;
- stato di avanzamento;
- criticità rilevate;
- eventuali scostamenti rispetto alle scadenze;
- evidenze documentali prodotte;
- rischi residui eventualmente accettati.

Per le azioni prioritarie sono inoltre registrati owner, rischio/gap di origine, riferimento alla valutazione dei rischi, indicatore di efficacia, data dell'ultima evidenza, dipendenze e motivazione degli scostamenti. Il RTD verifica che le azioni correttive siano attuate senza indebito ritardo e che nessuna azione sia chiusa sulla sola base di una dichiarazione priva di evidenze.

6. REPORTING AGLI ORGANI DI AMMINISTRAZIONE E DIRETTIVI

Con cadenza almeno semestrale viene predisposta una relazione contenente:

- stato di attuazione del Piano;
- interventi completati;
- interventi in corso;
- criticità rilevate;
- rischi residui significativi;
- proposte di ulteriori azioni di miglioramento.

Tale relazione è trasmessa agli organi di amministrazione e direttivi ai fini del monitoraggio dell'efficacia delle misure di sicurezza adottate.

Il reporting evidenzia separatamente le azioni scadute, i rischi elevati o non accettati, gli scostamenti di budget, le dipendenze da fornitori e le carenze che possono incidere sugli obblighi NIS2. Le decisioni, le priorità e le eventuali accettazioni del rischio residuo sono verbalizzate e ricondotte alla valutazione dei rischi.

L'Ente conserva le evidenze relative all'attuazione e al monitoraggio del Piano secondo le modalità definite dal proprio sistema documentale, al fine di assicurarne la tracciabilità e la disponibilità nell'ambito delle attività di audit, riesame e vigilanza

Gli esiti del monitoraggio che determinano una modifica significativa dell'esposizione al rischio sono recepiti nel processo di valutazione e trattamento del rischio del Comune di Parma, assicurando l'allineamento tra Piano di Adeguamento/Piano di trattamento.

7. RIESAME

Il Piano è riesaminato almeno annualmente e, ove necessario, aggiornato anche a seguito di:

- variazioni significative del contesto organizzativo o tecnologico;
- esiti della valutazione dei rischi;
- incidenti di sicurezza significativi;
- vulnerabilità rilevanti;
- audit e verifiche di conformità;
- modifiche normative o regolamentari;
- aggiornamenti delle misure ACN applicabili;
- modifiche rilevanti dei servizi affidati o della supply chain;
- risultati delle verifiche di efficacia delle misure;
- aggiornamenti rilevanti del SGSI di IT.CITY per i servizi ricadenti nel perimetro comunale.