Comune di Parma

RELAZIONE SULLO STATO DI ATTUAZIONE DEGLI OBBLIGHI PREVISTI DAL D.LGS. 138/2024 (NIS2), SULLA TUTELA DEI SISTEMI, DEI DATI E SULLA CONTINUITÀ OPERATIVA DEL COMUNE DI PARMA

OTTOBRE 2026

1 PREMESSA 4

PARTE I 4

2 "INTERVENTI, FORNITURE E SERVIZI REALIZZATI MEDIANTE FINANZIAMENTO ACN - PNRR MISURA 1.5 CYBERSECURITY" 4

2.1 Monitoraggio della sicurezza e Security Operations Center (SOC) 4
2.2 Governance, analisi della postura di sicurezza e pianificazione 4
2.3 Potenziamento della rete Wi-Fi e degli apparati di telecomunicazione 5
2.4 Firewall e controllo degli accessi alla rete mediante NAC 5
2.5 Protezione dei servizi online dagli attacchi DDoS 6
2.6 Assessment di Active Directory e formazione specialistica 6
2.7 Verifiche di sicurezza dei servizi web 6
2.8 Protezione e anonimizzazione dei dati 7
2.9 Servizi Microsoft 365 e sistemi di protezione cloud 7
2.10 Potenziamento del PAM e piattaforma di cybersecurity awareness 7
2.11 Endpoint protection, threat intelligence e aggiornamento SOAR 7

3 ULTERIORI INTERVENTI FINANZIATI CON RISORSE DEL BILANCIO COMUNALE 7

3.1 Interventi finanziati con risorse del Bilancio comunale 2026 7

PARTE II 8

4 STATO DI ATTUAZIONE DEGLI OBBLIGHI NIS2, RISULTATI RAGGIUNTI, RISCHI RESIDUI E PROSSIMI INTERVENTI 8

4.1 Finalità e chiave di lettura 8
4.2 Sintesi dello stato attuale 8
4.3 Quadro immediato per gli amministratori 9
4.3.1 Governance 9
4.3.2 Gestione del rischio 9
4.3.3 Gestione degli incidenti 9
4.3.4 Continuità operativa 9
4.3.5 Protezione tecnologica 9
4.3.6 Miglioramento 9

5 RISULTATI RAGGIUNTI 9

5.1 Sistema di gestione e governance della sicurezza 9
5.2 Valutazione e trattamento del rischio 9
5.3 Monitoraggio, vulnerabilità e risposta agli incidenti 10
5.4 Continuità operativa e capacità di ripristino 10
5.5 Efficacia della protezione dei servizi esposti su Internet 10
5.6 Risultati della protezione DDoS sintesii 11
5.7 Formazione e consapevolezza 11

6 RISCHI RESIDUI E LIMITI DA CONSIDERARE 11

6.1 Limite emerso nella protezione DDoS 11
6.2 Principali aree di rischio 12

7 PROSSIMI INTERVENTI 12

7.1 Interventi prioritari 12
7.2 Presidio e verifica nel tempo 13

8 VALUTAZIONE COMPLESSIVA (SINTESI) PER GLI ORGANI DI AMMINISTRAZIONE E DIRETTIVI 13

8.1 Sintesi 13
8.1.1 Risultati raggiunti 13

8.1.2 Rischi residui 14
8.1.3 Prossimi interventi 14

9 RIFERIMENTI NORMATIVI 14

1 Premessa

La presente relazione è predisposta ai fini dell'informazione agli Organi di Amministrazione e Direttivi del Comune di Parma sullo stato di attuazione degli obblighi derivanti dal D.Lgs. 138/2024, di recepimento della Direttiva (UE) 2022/2555 (NIS2), nonché sul livello di tutela dei sistemi informativi, dei dati e della continuità operativa dell'Ente.
La relazione si basa sulla documentazione SGSI predisposta dal Settore Sviluppo Economico e Transizione Digitale in collaborazione con la società partecipata IT.CITY S.p.A., sulla documentazione progettuale relativa agli interventi finanziati dall'Agenzia per la Cybersicurezza Nazionale, sulla documentazione progettuale relativa ad interventi finanziati con risorse del Bilancio Comunale, sulle valutazioni del rischio, sul Piano di Trattamento del Rischio, sul Piano di Adeguamento, sui piani di continuità operativa e disaster recovery e sulla documentazione tecnica disponibile agli atti dell'Ente

PARTE I

2 "Interventi, forniture e servizi realizzati mediante finanziamento ACN - PNRR Misura 1.5 Cybersecurity"

Nell'ambito del progetto "L'evoluzione della cyber security a 360°. Dalla formazione alle tecnologie innovative", finanziato dall'Agenzia per la Cybersicurezza Nazionale nell'ambito della Missione 1, Componente 1, Investimento 1.5 Cybersecurity del PNRR, il Comune di Parma ha attuato un programma integrato di rafforzamento della resilienza informatica, articolato in interventi di governance, protezione delle reti e dei dati, monitoraggio, continuità operativa, verifica tecnica e formazione.
La spesa complessivamente rendicontata ammonta a euro 1.298.379,64, rispetto a un finanziamento ammesso di euro 1.334.660,00. Di seguito sono riepilogati i servizi e le forniture acquisiti, con indicazione delle principali finalità di sicurezza.

2.1 Monitoraggio della sicurezza e Security Operations Center (SOC)

Nell'ambito del percorso di rafforzamento della sicurezza informatica avviato negli anni precedenti, il Comune di Parma aveva già attivato, a partire dal 2022, un servizio specialistico per il monitoraggio e la gestione degli incidenti, basato sulla piattaforma Certego Breach Detection & Incident Response (BDIR) e operante secondo il modello di Security Operations Center (SOC). Il servizio integrava la raccolta e correlazione degli eventi di sicurezza, il monitoraggio della rete e degli endpoint, l'analisi delle anomalie, la threat intelligence, l'investigazione degli incidenti e il supporto alle attività di contenimento e ripristino, rafforzando la capacità dell'Ente di individuare e gestire tempestivamente minacce e tentativi di compromissione.
Nel biennio 2024-2025 il presidio è stato ulteriormente consolidato attraverso la prosecuzione delle attività di monitoraggio, analisi degli eventi, gestione delle vulnerabilità e risposta agli incidenti. La quota riferita all'anno 2025, ammessa al finanziamento dell'Agenzia per la Cybersicurezza Nazionale, è risultata pari a euro 80.999,46, IVA inclusa. Le relative funzioni trovano continuità e ulteriore sviluppo nel successivo intervento di aggiornamento dei sistemi di Endpoint Protection, dei servizi di Threat Intelligence e della piattaforma SOAR, descritto nel prosieguo della relazione.

2.2 Governance, analisi della postura di sicurezza e pianificazione

IT.CITY S.p.A., in coordinamento con il Settore Transizione Digitale, ha assicurato la realizzazione della prima fase del progetto relativa alla governance e alla programmazione degli interventi di cybersicurezza, mediante l'attivazione di servizi specialistici affidati a operatori qualificati. Tale fase ha compreso l'analisi della postura di sicurezza dell'Ente, l'individuazione delle priorità di intervento, la definizione di un piano di potenziamento e il rafforzamento dei processi e degli assetti organizzativi preposti alla gestione della sicurezza informatica. L'importo complessivamente sostenuto per i predetti servizi è stato pari a euro 58.560,00, IVA inclusa.
Anche i servizi e le attività tecniche finalizzati all'aggiornamento della governance interna del sistema informatico e alla predisposizione della Business Impact Analysis (BIA), del Piano di continuità operativa e del Piano di Disaster Recovery sono stati affidati a IT.CITY S.p.A., che, per la loro realizzazione, si è avvalsa di operatori qualificati e specializzati nel settore della cybersicurezza.
La BIA ha consentito di individuare i processi e i servizi critici dell'Amministrazione comunale, di valutare gli impatti derivanti da una loro eventuale interruzione e di definire i relativi obiettivi e priorità di

ripristino. L'intervento, per un importo complessivo pari a euro 109.800,00, IVA inclusa, ha riguardato i seguenti processi essenziali, rappresentativi delle aree operative maggiormente sensibili:

- servizi di anagrafe e stato civile;
- servizi di protocollo;
- servizi di gestione del personale;
- servizi educativi.

Il processo di elaborazione della BIA si è articolato nelle seguenti fasi:

- Pianificazione e avvio, con la definizione degli obiettivi dell'analisi e l'individuazione del gruppo di progetto;
- Raccolta delle informazioni, mediante interviste e questionari rivolti ai responsabili delle funzioni interessate;
- Analisi degli impatti, attraverso la valutazione delle conseguenze derivanti dall'interruzione dei processi secondo differenti orizzonti temporali, tra cui 4, 24 e 72 ore;
- Determinazione dei parametri di continuità, con la definizione:
  - ✓ del Maximum Tolerable Downtime (MTD), corrispondente al periodo massimo di interruzione tollerabile;
  - ✓ del Recovery Time Objective (RTO), ossia il tempo entro il quale il processo deve essere ripristinato;
  - ✓ del Recovery Point Objective (RPO), che individua la massima perdita di dati ritenuta accettabile;
- Classificazione dei processi e definizione delle priorità, sulla base del relativo livello di criticità e delle esigenze di ripristino;
- Validazione e revisione degli esiti, finalizzate a verificarne la coerenza con l'organizzazione, i servizi erogati e le esigenze di continuità operativa dell'Ente.

2.3 Potenziamento della rete Wi-Fi e degli apparati di telecomunicazione

Nell'ambito degli interventi finalizzati al rafforzamento della sicurezza delle applicazioni, dei dati e delle reti, è stata realizzata la reingegnerizzazione e il potenziamento dell'infrastruttura Wi-Fi comunale, per un importo complessivo pari a euro 55.923,58, IVA inclusa.
L'intervento ha previsto la dismissione del controller non più supportato dal produttore, la sostituzione degli access point non più aggiornabili, l'ampliamento della copertura wireless nelle sedi comunali e l'installazione di un nuovo controller basato su tecnologia Fortinet. Sono stati complessivamente installati e configurati 86 access point, di cui 66 apparati wireless indoor tri-radio e 20 apparati FortiAP-U431F, estendendo in particolare la connettività presso il DUC, la Sede Municipale e la Casa della Musica.
A completamento dell'aggiornamento dell'infrastruttura di rete, sono stati inoltre acquisiti, installati e configurati nuovi apparati attivi di telecomunicazione, per un importo complessivo pari a euro 54.900,00, IVA inclusa. In particolare, la sostituzione degli switch, ossia degli apparati che collegano i dispositivi e gestiscono il traffico all'interno della rete locale, ha consentito di superare sulle sedi principali l'obsolescenza delle componenti esistenti e di adottare dispositivi conformi alle più recenti tecnologie e agli standard di sicurezza vigenti.

2.4 Firewall e controllo degli accessi alla rete mediante NAC

Nel corso del 2025 è stato completato il potenziamento delle misure di sicurezza perimetrale e di controllo degli accessi alla rete del Comune di Parma mediante l'installazione di nuovi apparati firewall Fortinet di classe enterprise e di una piattaforma di Network Access Control (NAC) HPE Aruba ClearPass. L'intervento ha consentito di rafforzare la protezione delle reti e dei sistemi informativi dell'Ente attraverso la segmentazione del traffico, l'applicazione delle politiche di sicurezza, il controllo degli accessi e il monitoraggio dei dispositivi connessi alla rete. In particolare, la soluzione NAC consente di verificare l'identità degli utenti e dei dispositivi prima dell'accesso alle risorse digitali, applicando regole differenziate in funzione del profilo di autorizzazione e dello stato di conformità degli apparati. L'implementazione della soluzione di Network Access Control (NAC) è attualmente in fase di completamento presso le sedi decentrate caratterizzate da un più elevato profilo di rischio, al fine di estendere in modo omogeneo i meccanismi di controllo, autenticazione e autorizzazione degli accessi alla rete comunale. L'infrastruttura realizzata rappresenta un elemento fondamentale per l'attuazione delle misure di sicurezza previste dal D.Lgs. 138/2024 e dalle Specifiche di Base ACN, contribuendo al rafforzamento della resilienza informatica dell'Ente.

2.5 Protezione dei servizi online dagli attacchi DDoS

Nell'ambito degli interventi finalizzati alla sicurezza delle applicazioni, dei dati e delle reti, è stata acquisita e installata una soluzione per il potenziamento della capacità di difesa dagli attacchi Distributed Denial of Service (DDoS), che possono compromettere la disponibilità dei servizi online mediante la saturazione delle risorse di rete o applicative. L'intervento, per un importo complessivo pari a euro 19.898,20, IVA inclusa, ha previsto l'integrazione di un'apposita appliance anti-DDoS nel sistema di protezione delle applicazioni web. Contestualmente è stato potenziato il sistema Web Application Firewall (WAF) mediante l'installazione di un secondo apparato in configurazione di alta affidabilità.
Il WAF è una soluzione specificamente destinata a controllare e proteggere il traffico diretto verso le applicazioni web, contribuendo a prevenire accessi e richieste potenzialmente dannosi. La configurazione in alta affidabilità assicura la continuità del presidio anche in caso di indisponibilità di uno dei componenti. L'intervento ha rafforzato l'affidabilità dell'infrastruttura e la protezione dei servizi digitali dell'Ente, riducendo il rischio di interruzioni derivanti da guasti, compromissioni o attacchi informatici.

2.6 Assessment di Active Directory e formazione specialistica

Nell'ambito degli interventi finalizzati al rafforzamento della gestione delle identità digitali e delle competenze specialistiche dell'Ente, sono stati realizzati un assessment di sicurezza di Active Directory e un percorso formativo rivolto al personale IT, per un importo complessivo pari a euro 91.500,00, IVA inclusa. L'assessment effettuato mediante l'attivazione di servizi specialistici affidati a operatori qualificati, ha consentito di verificare le configurazioni e le autorizzazioni dell'ambiente Active Directory e si è concluso con la redazione di una relazione di Vulnerability Assessment e con il potenziamento dei controlli diretti a prevenire accessi non autorizzati, violazioni dei dati e compromissioni di informazioni sensibili. La formazione, articolata in attività teoriche e pratiche, ha approfondito la gestione degli incidenti, lo sviluppo sicuro del codice e la sicurezza dei sistemi di pubblicazione, rafforzando le capacità operative di rilevazione e risposta agli eventi informatici

2.7 Verifiche di sicurezza dei servizi web

Nell'ambito degli interventi finalizzati all'analisi della postura di sicurezza e alla protezione delle applicazioni, dei dati e delle reti, è stato completato un processo di Web Application Penetration Test sui principali servizi web del Comune di Parma, per un importo complessivo pari a euro 61.000,00, IVA inclusa.
Il Penetration Test consiste in una verifica tecnica controllata, condotta simulando il punto di vista di un potenziale attaccante, finalizzata a individuare eventuali vulnerabilità applicative, verificare l'efficacia delle misure di protezione adottate e valutare le possibili conseguenze derivanti dallo sfruttamento delle criticità rilevate.
L'attività ha interessato i seguenti servizi:

- Sistema gestionale dei servizi demografici piattaforma denominata J-Demos Evo;
- Portale web dei certificati;
- Sistema gestionale dei servizi di welfare denominato Icaro Evo;
- Sistema di gestione del personale denominato GipsiPortal;
- Sistema di erogazione dei servizi online denominato ElixForm;
- Sistemi on line di prenotazione ai servizi comunali "Agenda";
- Sistema per la gestione del servizio elettorale compreso i sistemi di rilevazione dei dati di scrutinio (comunicazioni elettorali).

Per ciascun servizio sono stati definiti la tipologia di verifica da effettuare, secondo modalità Black Box o Gray Box, e l'ambito applicativo da sottoporre ad analisi. Le verifiche hanno consentito di valutare il livello di sicurezza delle applicazioni rispetto a un attaccante esterno alla rete, misurare il rischio effettivo delle piattaforme in uso e individuare i possibili impatti per l'Ente.
Per ciascun servizio analizzato è stato predisposto uno specifico rapporto nel quale le vulnerabilità riscontrate sono state classificate in base alla severità e alla priorità di intervento. Gli esiti hanno consentito di individuare le azioni necessarie alla mitigazione dei rischi e alla risoluzione delle vulnerabilità rilevate.

2.8 Protezione e anonimizzazione dei dati

Nell'ambito delle attività dedicate alla sicurezza delle applicazioni, dei dati e delle reti, è stato acquisito e implementato un sistema cloud per l'anonimizzazione delle informazioni strutturate e non strutturate, per un importo complessivo pari a euro 122.000,00, IVA inclusa.
La soluzione INFORMATICA IDMC è stata configurata ed è operativa. Il sistema è finalizzato alla trasformazione e alla protezione delle informazioni, in modo da ridurre, secondo le funzionalità e le modalità di trattamento applicate, la possibilità di ricondurre i dati a soggetti identificati o identificabili. L'intervento rafforza quindi i presìdi di sicurezza e riservatezza dei dati trattati dall'Amministrazione e si inserisce nel più ampio programma di protezione delle informazioni e degli ambienti cloud.

2.9 Servizi Microsoft 365 e sistemi di protezione cloud

Sono state acquisite licenze Microsoft 365 e implementate soluzioni cloud per rafforzare la protezione dei dati non strutturati e della posta elettronica. L'intervento, del valore complessivo di euro 48.800,00, IVA inclusa, è stato completato e si integra con le ulteriori misure di protezione degli endpoint descritte nel prosieguo della relazione

2.10 Potenziamento del PAM e piattaforma di cybersecurity awareness

Sono stati completati il potenziamento del sistema Privileged Access Management (PAM) NETWRIX e il percorso di sensibilizzazione del personale in materia di cybersicurezza, per un importo complessivo pari a euro 70.760,00, IVA inclusa.
Il potenziamento del PAM ha consentito di estendere e rendere pienamente operativo il controllo degli accessi privilegiati alle risorse critiche dell'Ente, anche da parte dei fornitori, sostituendo gli accessi remoti standard con modalità più sicure e controllate. Sono state inoltre concluse le relative sessioni formative.
Il percorso di cybersecurity awareness, (CyberGuru) tuttora in corso, prevede corsi in modalità FAD, simulazioni di phishing e campagne interne multicanale sui principali rischi informatici, sulla protezione dei dati e dei dispositivi e sui comportamenti corretti da adottare. Si auspica che le iniziative finora attuate producano effetti positivi e duraturi sul livello di consapevolezza del personale, contribuendo al contenimento del rischio umano, al corretto utilizzo delle credenziali di accesso e al rafforzamento complessivo della postura di sicurezza dell'Ente.

2.11 Endpoint protection, threat intelligence e aggiornamento SOAR

Nell'ambito del percorso di rafforzamento della postura di sicurezza dell'Ente sono state implementate ulteriori misure finalizzate alla protezione delle postazioni di lavoro e dei dispositivi terminali, al miglioramento delle capacità di analisi delle minacce informatiche e all'evoluzione dei processi di monitoraggio e risposta agli eventi di sicurezza. In particolare, sono state estese le funzionalità di Endpoint Protection per la prevenzione, il rilevamento e il contenimento delle minacce sugli endpoint, potenziati i servizi di Threat Intelligence per l'acquisizione e la correlazione di informazioni relative a vulnerabilità, campagne malevole e indicatori di compromissione, nonché aggiornati i sistemi di Security Orchestration, Automation and Response (SOAR), finalizzati all'automazione dei flussi di gestione e risposta agli incidenti di sicurezza. Tali interventi contribuiscono a migliorare le capacità di individuazione precoce delle minacce, di analisi degli eventi e di coordinamento delle azioni di risposta, rafforzando complessivamente la resilienza dei sistemi informativi dell'Ente e la capacità di gestione degli incidenti prevista dal Sistema di Gestione della Sicurezza delle Informazioni (SGSI) e dal quadro degli obblighi introdotti dal D.Lgs. 138/2024.

3 Ulteriori interventi finanziati con risorse del Bilancio comunale

Concluso il progetto finanziato dall'Agenzia per la Cybersicurezza Nazionale, il Comune di Parma ha programmato ulteriori interventi di consolidamento della sicurezza informatica, sostenuti con risorse del Bilancio comunale 2026.

3.1 Interventi finanziati con risorse del Bilancio comunale 2026

In continuità con le attività già realizzate nell'ambito del progetto finanziato dall'Agenzia per la Cybersicurezza Nazionale, il Comune di Parma ha programmato ulteriori interventi di consolidamento e sviluppo della sicurezza informatica. Tali attività non rientrano nel progetto ACN, concluso il 31 marzo 2026, ma sono finanziate con risorse proprie del Bilancio comunale 2026.

Nell'ambito dei servizi erogati da IT.CITY S.p.A. è stato previsto il rinnovo della manutenzione del sistema A10 Network TPS (Threat Protection System), attivato nel 2025 per la difesa dagli attacchi DDoS. La soluzione filtra il traffico di rete, consentendo il transito di quello legittimo e bloccando quello malevolo, e concorre a garantire la sicurezza perimetrale e la disponibilità dei servizi digitali dell'Ente.
Sono stati inoltre finanziati, per un importo complessivo di euro 45.556,02, IVA inclusa, ulteriori servizi per l'attuazione degli obblighi NIS2. Gli interventi comprendono la predisposizione del Piano della Sicurezza 2026-2028, attività per la dismissione o l'aggiornamento dei sistemi giunti a fine vita, la segregazione degli ambienti di produzione, test e sviluppo, nonché l'evoluzione dell'infrastruttura del data center. Sono altresì previsti percorsi formativi specialistici rivolti agli organi di amministrazione e direttivi e al personale dell'Ente, oltre all'avvio di un processo strutturato di gestione dei rischi connessi alla catena di fornitura e ai soggetti terzi che contribuiscono all'erogazione dei servizi digitali comunali.
Le attività sono finanziate sul capitolo del Bilancio 2026 dedicato alle spese per la sicurezza informatica.

PARTE II

4 Stato di attuazione degli obblighi NIS2, risultati raggiunti, rischi residui e prossimi interventi

4.1 Finalità e chiave di lettura

La presente Parte II fornisce agli organi di amministrazione e direttivi un quadro sintetico e comprensibile dello stato di attuazione degli obblighi previsti dal D.Lgs. 138/2024. La relazione evidenzia le misure già adottate, gli effetti prodotti sulla protezione dei servizi comunali, i rischi che permangono e gli interventi necessari per consolidare nel tempo il livello di sicurezza raggiunto.
La sicurezza informatica non riguarda soltanto le tecnologie. Essa incide direttamente sulla continuità dei servizi ai cittadini, sulla tutela dei dati, sull'operatività degli uffici e sulla capacità dell'Ente di reagire a guasti, attacchi e situazioni di crisi. **Per tale ragione, il percorso NIS2 è stato impostato come un processo permanente di governo del rischio e di miglioramento continuo**.

4.2 Sintesi dello stato attuale

L'assessment condotto nell'ambito del progetto PNRR Avviso n. 8/2024 dell'Agenzia per la Cybersicurezza Nazionale, secondo una metodologia riconosciuta a livello internazionale, ha esaminato 117 aspetti della sicurezza informatica. Di questi, 88, pari al 75%, risultavano già a regime, mentre 21 erano in corso di completamento.
Tra i principali presìdi già operativi rientravano il monitoraggio continuativo dei sistemi, l'autenticazione a più fattori, il controllo degli accessi dei fornitori, la protezione degli endpoint, i sistemi di backup e ripristino e le attività formative. Le principali azioni di consolidamento riguardano l'estensione della Business Impact Analysis oltre i primi processi prioritari, il rafforzamento delle verifiche sui fornitori, l'esecuzione dei test di sicurezza, l'aggiornamento dei sistemi obsoleti e il riesame periodico dei diritti di accesso.
Sulla base degli esiti dell'assessment, il Comune di Parma ha adottato un proprio modello organizzativo per la gestione della sicurezza delle informazioni, nell'ambito del quale sono definiti ruoli, responsabilità, funzioni di governo, indirizzo, supervisione e controllo in materia di sicurezza delle informazioni e cybersicurezza ai fini dell'adeguamento al D.Lgs. 138/2024 e alle Specifiche di base ACN.
Nell'ambito 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 e misure di sicurezza definite e attuate dalla società, quale riferimento per la gestione operativa della sicurezza delle informazioni e dei sistemi informativi.

Alla data della presente relazione risultano completate le principali attività di definizione dell'assetto organizzativo e documentale. Sono inoltre operative misure tecnologiche per il monitoraggio continuo, la protezione delle reti e degli endpoint, il controllo degli accessi, il backup e il ripristino dei dati e la difesa dei servizi pubblicati su Internet.
Le attività ancora da consolidare sono state individuate nell'ambito della valutazione del rischio e ricondotte al Piano di trattamento del rischio e al Piano di adeguamento dell'Ente, che ne definiscono priorità e modalità di attuazione.

4.3 Quadro immediato per gli amministratori

4.3.1 Governance

Ruoli, responsabilità e rapporti tra Comune e IT.CITY S.p.A. sono definiti; le funzioni di indirizzo, approvazione, supervisione e vigilanza restano in capo al Comune.

4.3.2 Gestione del rischio

È stata completata la valutazione dei principali sistemi ed è stato predisposto il Piano di trattamento, nel quale sono individuate azioni, responsabilità e scadenze.

4.3.3 Gestione degli incidenti

È disponibile una procedura strutturata che disciplina la rilevazione, la classificazione, l'escalation, la conservazione delle evidenze e le notifiche verso l'Agenzia per la Cybersicurezza Nazionale e CSIRT Italia.

4.3.4 Continuità operativa

Sono stati predisposti i Piani di Business Continuity e Disaster Recovery e sono operative soluzioni di replica tra i Data Center di Parma e Ferrara.

4.3.5 Protezione tecnologica

Sono attivi firewall, sistemi NAC, servizi SOC, strumenti di protezione degli endpoint e degli ambienti cloud, attività di vulnerability assessment, sistemi di backup e soluzioni di protezione dagli attacchi DDoS.

4.3.6 Miglioramento

Sono pianificati ulteriori interventi riguardanti la gestione degli accessi, la sicurezza dei fornitori, il trattamento delle vulnerabilità, la protezione delle reti e delle applicazioni, la Business Impact Analysis, i sistemi di backup e i controlli sugli ambienti cloud.

5 Risultati raggiunti

5.1 Sistema di gestione e governance della sicurezza

È stato predisposto il corpus documentale richiesto dalle misure di sicurezza di base dell'Agenzia per la Cybersicurezza Nazionale, comprendente:

- l'organizzazione per la sicurezza informatica;
- le politiche di sicurezza;
- il processo di valutazione e trattamento del rischio;
- la gestione delle vulnerabilità;
- il Piano di adeguamento;
- il Piano di continuità operativa;
- il Piano di disaster recovery;
- il Piano di gestione delle crisi informatiche;
- il Piano di formazione e sensibilizzazione;
- il Piano e la procedura per la gestione degli incidenti di sicurezza informatica.

Il framework è articolato in politiche, procedure, istruzioni operative e registrazioni, così da rendere verificabili le responsabilità attribuite, le attività svolte e le decisioni assunte.
Il modello organizzativo individua gli organi di amministrazione e direttivi, il Responsabile per la Transizione Digitale, il Punto di Contatto NIS, il Referente CSIRT, il Comitato di crisi, il gruppo di gestione degli incidenti, il Security Operations Center e le figure tecniche coinvolte.
IT.CITY S.p.A. assicura il supporto e l'attuazione operativa del SGSI, mentre le funzioni di indirizzo, approvazione, supervisione e vigilanza restano in capo al Comune di Parma.

5.2 Valutazione e trattamento del rischio

È stata completata la valutazione del rischio mediante la metodologia VERA 8.0. L'analisi ha incluso, tra gli altri, Microsoft 365, Active Directory, il protocollo informatico Engramma, i sistemi del personale, i firewall, i sistemi di monitoraggio e backup, le piattaforme cloud e le infrastrutture di rete e sicurezza.

Gli esiti della valutazione sono confluiti nel Piano di trattamento del rischio, che associa alle criticità rilevate specifiche misure di mitigazione, soggetti responsabili e scadenze.
Tale impostazione consente agli organi dell'Ente di disporre di una base strutturata per:

- individuare i rischi maggiormente rilevanti;
- definire le priorità di intervento;
- verificare lo stato di avanzamento delle misure;
- valutare il rischio residuo;
- indirizzare le risorse verso gli interventi maggiormente efficaci.

5.3 Monitoraggio, vulnerabilità e risposta agli incidenti

Sono operative attività di monitoraggio e scansione delle vulnerabilità mediante strumenti specialistici, tra cui Nessus, e sistemi SOC centralizzati.
Il Piano di gestione delle vulnerabilità disciplina:

- il monitoraggio dei bollettini di sicurezza;
- la rilevazione delle vulnerabilità;
- la valutazione della loro gravità;
- la definizione delle priorità di intervento;
- la remediation;
- il patch management;
- le attività di threat intelligence;
- la verifica dell'effettiva risoluzione delle criticità.

La procedura di gestione degli incidenti disciplina l'intero ciclo di risposta, comprendente:

- rilevazione e segnalazione;
- classificazione;
- gestione operativa;
- escalation;
- contenimento;
- ripristino;
- conservazione delle evidenze;
- gestione degli eventuali data breach;
- rapporti con ACN e CSIRT Italia;
- attivazione della gestione di crisi;
- analisi successiva all'incidente e individuazione delle azioni di miglioramento.

Sono recepiti i termini previsti dalla disciplina NIS2 per la pre-notifica entro 24 ore, la notifica entro 72 ore e la trasmissione della relazione finale entro un mese.

5.4 Continuità operativa e capacità di ripristino

Sono stati predisposti il Piano di Business Continuity e il Piano di Disaster Recovery.
L'architettura si basa sul Data Center primario Lepida di Parma e sul Data Center secondario Lepida di Ferrara, con meccanismi di replica realizzati mediante:

- VMware Site Recovery;
- Oracle Data Guard;
- Microsoft SQL Log Shipping;
- replica dei dati non strutturati.

Sono stati individuati processi critici e obiettivi di ripristino per il protocollo informatico, i servizi demografici, il personale e i servizi educativi.
Tali misure riducono il rischio che un guasto, un attacco informatico o un'indisponibilità infrastrutturale determini un'interruzione prolungata delle funzioni istituzionali dell'Ente.

5.5 Efficacia della protezione dei servizi esposti su Internet

La protezione dagli attacchi DDoS offre un riscontro concreto dell'efficacia degli investimenti effettuati.
Nel periodo compreso tra il 15 giugno 2025 e il 19 agosto 2026, la piattaforma A10 Thunder TPS ha protetto 8 zone infrastrutturali e 30 servizi tecnici, attraverso i quali risultano pubblicati circa 300 siti e servizi web.
Nel medesimo periodo la piattaforma ha:

- registrato 1.888 incidenti;
- analizzato circa 9,81 miliardi di pacchetti;

- scartato circa 938 milioni di pacchetti non conformi alle politiche di sicurezza configurate.

Gli attacchi infrastrutturali maggiormente significativi hanno raggiunto durate superiori alle 20 e alle 25 ore.
Nei principali casi documentati il portale istituzionale è rimasto disponibile mentre il sistema rilevava l'anomalia, applicava le contromisure e continuava a inoltrare il traffico ritenuto ammissibile.
L'assenza di un disservizio percepibile non indica, pertanto, l'assenza di attacchi, ma costituisce, nei casi documentati, un risultato coerente con l'efficacia delle misure adottate e con le attività tecniche di monitoraggio e gestione.

5.6 Risultati della protezione DDoS sintesii

Circa 300 siti e servizi web inclusi nel perimetro
La protezione riguarda un insieme ampio di servizi digitali esposti a cittadini, imprese e uffici comunali.
Attacchi di durata superiore alle 20 e alle 25 ore
Il presidio ha mantenuto operative le contromisure durante campagne prolungate e ripetute.
Fino a circa 211,98 milioni di pacchetti scartati in un singolo evento documentato
Una quantità rilevante di traffico anomalo non è stata inoltrata ai sistemi applicativi dell'Ente.
Portale disponibile durante i principali attacchi infrastrutturali
Le misure adottate hanno contribuito alla continuità del servizio durante gli eventi compresi nel perimetro di rilevazione della piattaforma.
Produzione di report strutturati e conservazione delle evidenze
L'Ente può ricostruire gli eventi, verificare l'efficacia delle contromisure adottate e disporre di elementi documentali utili per il reporting, gli audit e le attività di vigilanza.

5.7 Formazione e consapevolezza

È stato predisposto un Piano di formazione rivolto:
- agli organi di amministrazione e direttivi;
- ai dirigenti;
- al personale dell'Ente;
- agli amministratori di sistema;
- al Punto di Contatto NIS;
- al Referente CSIRT;
- ai fornitori e ai collaboratori coinvolti nella gestione dei sistemi informativi.

I percorsi riguardano, in particolare, la disciplina NIS2, la gestione degli incidenti, il phishing, la protezione dei dati, la continuità operativa e la gestione delle vulnerabilità.
Ci si attende che le attività già realizzate favoriscano il progressivo rafforzamento della consapevolezza del personale e contribuiscano alla riduzione dei rischi connessi all'uso improprio delle credenziali, dei sistemi e delle risorse digitali dell'Ente.

6 Rischi residui e limiti da considerare

Il livello di protezione raggiunto non elimina il rischio informatico.
La sicurezza dipende dall'integrazione tra organizzazione, tecnologie, procedure, competenze e controllo continuo. Nessun singolo presidio tecnologico è in grado di coprire ogni possibile modalità di attacco.

6.1 Limite emerso nella protezione DDoS

Il 18 dicembre 2025 il portale istituzionale ha subito un attacco applicativo basato su richieste HTTPS formalmente valide.
Il traffico imitava il comportamento di numerosi utenti legittimi e non ha attivato automaticamente le contromisure del sistema TPS, determinando disservizi.
L'episodio non riduce l'efficacia dimostrata dalla piattaforma contro gli attacchi infrastrutturali, ma ne chiarisce il perimetro operativo e conferma la necessità di una difesa multilivello composta da:
- sistema TPS;
- reverse proxy;
- script aFleX;
- Web Application Firewall;
- meccanismi di rate limiting;
- monitoraggio applicativo;

- intervento tecnico specialistico.

6.2 Principali aree di rischio

Gestione degli accessi
Diritti di accesso non più necessari o non riesaminati periodicamente possono favorire accessi impropri a sistemi e informazioni.

Fornitori e catena di approvvigionamento
Una vulnerabilità tecnica o una carenza organizzativa di un fornitore critico può riflettersi sui sistemi e sui servizi comunali.

Vulnerabilità e aggiornamenti
Ritardi nelle attività di remediation o la presenza di sistemi non più supportati dai produttori possono lasciare esposte vulnerabilità note.

Reti e accesso dei dispositivi
La segmentazione delle reti e il controllo degli accessi devono essere completati e mantenuti coerenti con l'evoluzione dell'infrastruttura.

Sicurezza applicativa
Occorre consolidare le verifiche sul software sviluppato o acquisito e rafforzare la protezione dei dati utilizzati negli ambienti di test.

Continuità operativa
La Business Impact Analysis deve essere estesa per definire in modo completo le priorità e i tempi di ripristino dei servizi dell'Ente.

Attacchi applicativi e DDoS
Richieste apparentemente legittime possono eludere i controlli infrastrutturali. Le soglie, il perimetro e i controlli complementari devono quindi essere riesaminati periodicamente.

Competenze e capacità operativa
L'efficacia dei presidi dipende dalla disponibilità continuativa di personale e fornitori dotati di competenze specialistiche.

7 Prossimi interventi

Le attività successive devono concentrarsi sulle aree già individuate nel Piano di trattamento del rischio e nel Piano di adeguamento, privilegiando gli interventi che riducono maggiormente l'impatto potenziale sui servizi essenziali e quelli direttamente collegati agli obblighi NIS2.

7.1 Interventi prioritari

Gli interventi prioritari riguardano:

- il completamento della Business Impact Analysis, estendendo la valutazione dei servizi critici e definendo l'ordine e i tempi di ripristino;
- la formalizzazione e l'attuazione del riesame periodico dei diritti di accesso;
- il rafforzamento del governo degli accessi privilegiati;
- il rafforzamento della sicurezza della catena di fornitura, mediante revisione contrattuale, monitoraggio dei fornitori critici e verifiche periodiche;
- la sostituzione o l'aggiornamento dei sistemi non più supportati dai produttori;
- il consolidamento dei processi di patch management dei server;
- il potenziamento del vulnerability management mediante scansioni continue, definizione delle priorità di remediation e controlli SAST, DAS[1]T e penetration test;
- il completamento del Network Access Control;
- il miglioramento della segregazione delle reti e delle postazioni;
- l'aggiornamento delle piattaforme di backup;
- il mantenimento di copie offline protette dagli attacchi ransomware e dall'indisponibilità dei sistemi primari;

[1] **SAST (Static Application Security Testing)** è un'analisi del software effettuata esaminando il codice applicativo prima della messa in esercizio o durante lo sviluppo. Consente di individuare errori di programmazione, vulnerabilità e pratiche non sicure direttamente nel codice sorgente.
· **DAST (Dynamic Application Security Testing)** è invece un'analisi eseguita sull'applicazione in esercizio o in ambiente di test. Simula il comportamento di un utente o di un attaccante esterno, verificando il funzionamento reale dell'applicazione e individuando eventuali vulnerabilità sfruttabili.

- il rafforzamento dei controlli applicativi e della protezione anti-DDoS mediante il riesame delle soglie e del perimetro di protezione;
- il potenziamento del Web Application Firewall, del rate limiting, degli script aFleX e del monitoraggio delle risorse applicative;
- la prosecuzione del potenziamento del SOC, dei servizi di threat intelligence, dell'automazione della risposta e dei controlli cloud e Data Loss Prevention;
- il mantenimento del programma di formazione, comprendente esercitazioni e aggiornamenti rivolti agli organi, al personale e alle figure tecniche.

7.2 Presidio e verifica nel tempo

Gli interventi tecnologici non possono essere considerati conclusi con l'acquisizione delle soluzioni.
Il mantenimento della loro efficacia richiede:

- manutenzione periodica;
- aggiornamento delle configurazioni;
- monitoraggio continuativo;
- analisi degli eventi;
- verifica delle prestazioni;
- conservazione delle evidenze;
- disponibilità di competenze adeguate.

Dovranno essere assicurati il riesame periodico dello stato di attuazione, la verifica dell'efficacia delle misure, l'aggiornamento della valutazione del rischio e la rendicontazione agli organi di amministrazione e direttivi.
Le modifiche sostanziali agli indirizzi strategici e al modello di governance resteranno sottoposte agli organi competenti, mentre gli aggiornamenti tecnico-gestionali dovranno garantire l'allineamento continuo del SGSI all'evoluzione dei rischi, delle minacce e delle tecnologie.

8 Valutazione complessiva (sintesi) per gli organi di amministrazione e direttivi

Il Comune di Parma dispone oggi di un impianto organizzativo e documentale SGSI, di una valutazione del rischio formalizzata, di processi strutturati per la gestione degli incidenti, della continuità operativa e del disaster recovery, nonché di misure tecnologiche che hanno già prodotto evidenze concrete di protezione e continuità dei servizi.
Il risultato raggiunto è significativo, ma non definitivo.
Permangono rischi residui e attività di consolidamento che richiedono priorità, risorse, controllo sull'avanzamento e riesame periodico.
In particolare, devono essere completati o rafforzati:

- la Business Impact Analysis;
- la verifica della sicurezza dei fornitori;
- il riesame periodico degli accessi;
- gli interventi sui sistemi obsoleti;
- il vulnerability management;
- la protezione applicativa;
- la protezione dagli attacchi DDoS di livello applicativo;
- il monitoraggio e la capacità di risposta agli incidenti;
- la formazione e la sensibilizzazione del personale.

Gli organi di amministrazione e direttivi sono pertanto chiamati a mantenere l'indirizzo e la supervisione sul percorso, verificando che le azioni pianificate siano attuate, che i rischi più rilevanti siano trattati con priorità e che il livello di protezione rimanga adeguato all'evoluzione delle minacce e dei servizi digitali dell'Ente.

8.1 Sintesi

8.1.1 Risultati raggiunti

Sono stati predisposti il SGSI, il modello di governance, la valutazione del rischio, la procedura di gestione degli incidenti, i piani di continuità operativa e disaster recovery. Sono inoltre operative misure

tecnologiche di protezione e monitoraggio, tra cui il SOC e il sistema di protezione DDoS, la cui efficacia risulta documentata negli eventi infrastrutturali analizzati.

8.1.2 Rischi residui

Devono essere ulteriormente consolidati la gestione degli accessi e dei fornitori, il trattamento delle vulnerabilità, l'aggiornamento dei sistemi obsoleti e la Business Impact Analysis. Permane inoltre il rischio rappresentato dagli attacchi applicativi non intercettabili dal solo sistema TPS e la necessità di assicurare continuativamente competenze specialistiche.

8.1.3 Prossimi interventi

Il percorso di adeguamento richiede il completamento e il consolidamento di ulteriori misure organizzative e tecnologiche, già individuate nell'ambito della valutazione del rischio e del Piano di adeguamento. Gli interventi programmati riguardano, in particolare, l'estensione della Business Impact Analysis (BIA) ad altri servizi rilevanti dell'Ente, il completamento del Network Access Control (NAC), il rafforzamento dei controlli sulla catena di fornitura, l'aggiornamento dei sistemi giunti a fine vita e il potenziamento delle capacità di backup, gestione delle vulnerabilità e verifica della sicurezza applicativa. Sono pertanto in corso di definizione i seguenti progetti, i cui importi definitivi saranno determinati a seguito dell'acquisizione delle relative offerte:

- Completamento della BIA, mediante l'estensione dell'analisi ad altri servizi rilevanti, tra cui atti amministrativi, Polizia Locale e servizi sociali, al fine di individuare le priorità e i tempi di ripristino in caso di interruzione;
- sostituzione o aggiornamento dei sistemi obsoleti, non più supportati dai produttori,
- aggiornamento del sistema di backup su nastro, per assicurare la disponibilità di copie offline non direttamente raggiungibili dalla rete e, pertanto, maggiormente protette rispetto ad attacchi ransomware;
- verifica della sicurezza dei fornitori ICT, mediante questionari e attività di analisi rivolti ai soggetti più rilevanti per l'erogazione dei servizi digitali, al fine di rafforzare la gestione dei rischi connessi alla catena di approvvigionamento; (attività già finanziata ed in corso di realizzazione)
- adozione di una soluzione cloud per il vulnerability management, finalizzata all'esecuzione continuativa delle scansioni, alla produzione di report e alla definizione delle priorità di mitigazione delle vulnerabilità individuate;
- gestione centralizzata degli aggiornamenti dei server Windows e Linux, allo scopo di rendere più tempestiva e uniforme l'installazione degli aggiornamenti di sicurezza;
- esecuzione periodica di penetration test, attraverso simulazioni controllate di attacco sui servizi online, con una programmazione indicativa di dieci servizi nell'arco di tre anni;
- introduzione di controlli DAST, ossia verifiche automatizzate effettuate sulle applicazioni durante il loro funzionamento, finalizzate a individuare errori e vulnerabilità nelle funzionalità e nelle interfacce dei servizi online, su un perimetro previsto di cento elementi.

La priorità più elevata è attribuita agli interventi che consentono di ridurre gli effetti di un'eventuale indisponibilità dei servizi o di un attacco informatico, quali il completamento della BIA, l'aggiornamento dei sistemi obsoleti e il rafforzamento delle copie di sicurezza offline, nonché alla verifica dei fornitori, espressamente rilevante ai fini della gestione del rischio della catena di approvvigionamento. Gli ulteriori interventi di vulnerability management, patch management e verifica applicativa sono classificati come priorità intermedia e sono destinati a rendere continuativo e strutturato il processo di individuazione, classificazione e correzione delle vulnerabilità.
Ciascun progetto concorre all'attuazione degli obblighi previsti dalla disciplina NIS2 e dei controlli del Sistema di Gestione della Sicurezza delle Informazioni. In particolare, gli interventi sono finalizzati a ridurre i rischi derivanti dall'interruzione dei servizi essenziali, dall'utilizzo di sistemi non più supportati, dalla compromissione delle copie di sicurezza, dagli accessi attraverso fornitori, dalla mancata individuazione delle vulnerabilità e dalla presenza di errori di sicurezza nei servizi digitali.

9 Riferimenti normativi

Il percorso di adeguamento del Comune di Parma si inserisce nel quadro delineato dalla Direttiva (UE) 2022/2555 (NIS2) e dal relativo decreto di recepimento, D.Lgs. 4 settembre 2024, n. 138, che attribuisce agli organi di amministrazione e direttivi specifiche responsabilità di approvazione e supervisione, disciplina le misure di gestione dei rischi per la sicurezza informatica e stabilisce gli obblighi di notifica degli incidenti significativi. [normattiva.it], [dleib_NIS_..._3516_2026 | Word]

Le modalità di attuazione sono definite dalla Determinazione ACN n. 379907/2025, applicabile dal 15 gennaio 2026, che aggiorna la precedente Determinazione n. 164179/2025 e individua le misure di sicurezza di base da adottare entro ottobre 2026, organizzate secondo il Framework nazionale per la Cybersecurity e la Data Protection. [acn.gov.it], [acn.gov.it], [acn.gov.it]
Il quadro di riferimento è completato dalla Legge 28 giugno 2024, n. 90, dal Codice dell'amministrazione digitale, dalle misure di sicurezza ICT per le pubbliche amministrazioni e dagli indirizzi del Piano triennale per l'informatica nella PA. Per quanto riguarda la protezione dei dati personali trovano inoltre applicazione il Regolamento (UE) 2016/679 e il D.Lgs. 196/2003, con particolare riferimento alla sicurezza dei trattamenti, alla protezione dei dati fin dalla progettazione, ai rapporti con i responsabili del trattamento e alla gestione delle violazioni dei dati personali.
Il Sistema di Gestione della Sicurezza delle Informazioni è stato sviluppato tenendo conto degli standard ISO/IEC 27001:2022 e ISO/IEC 27002:2022, mentre le attività di assessment e il conseguente percorso di miglioramento sono stati sostenuti dal PNRR, Missione 1, Componente 1, Investimento 1.5 "Cybersecurity", Avviso pubblico ACN n. 8/2024. Nel loro insieme, tali riferimenti costituiscono il quadro normativo, tecnico e organizzativo entro il quale l'Ente assicura la tutela dei sistemi informativi e di rete, dei dati e della continuità operativa dei servizi.