

Comune di Parma

Valutazione dei rischi per la sicurezza dei sistemi informativi e di rete

Documento per approvazione formale ai fini ID.RA-05

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

1 INTRODUZIONE 5
2 SCOPO E CAMPO DI APPLICAZIONE 5
3 RIFERIMENTI NORMATIVI E DOCUMENTALI 6
4 RUOLI E RESPONSABILITA' 7
5 PROCESSO DI VALUTAZIONE E TRATTAMENTO DEL RISCHIO 7
5.1 CRITERI PER L'ESECUZIONE DELLA VALUTAZIONE DEL RISCHIO 9
5.2 CRITERI DI ACCETTAZIONE DEL RISCHIO 9
5.3 FLUSSO DEL PROCESSO DI VALUTAZIONE E TRATTAMENTO DEI RISCHI 9
5.4 DETERMINAZIONE DEL CONTESTO 10
5.5 IDENTIFICAZIONE DEI RISCHI 11
5.5.1 IDENTIFICAZIONE DEGLI ASSET 11
5.5.2 IDENTIFICAZIONE DELLE POSSIBILI MINACCE 12
5.5.3 VALUTAZIONE DELLE VULNERABILITÀ E DEI CONTROLLI DI SICUREZZA IN ESSERE 12
5.5.4 IDENTIFICAZIONE DEGLI SCENARI DI RISCHIO 12
5.6 ANALISI DEL RISCHIO 12
5.6.1 CRITERI DI VALUTAZIONE DELLE INFORMAZIONI 13
5.6.2 IDENTIFICAZIONE E VALUTAZIONE DELLE MINACCE 14
5.6.3 VALUTAZIONE EFFICACIA DEI CONTROLLI DELLA ISO/IEC 27001:2022 14
5.6.4 CLASSIFICAZIONE DEL RISCHIO 15
5.7 PONDERAZIONE DEL RISCHIO 15
5.7.1 REPORT DI VALUTAZIONE DEL RISCHIO 16
5.8 TRATTAMENTO DEL RISCHIO 16
5.8.1 OPZIONI DI TRATTAMENTO DEL RISCHIO 16
5.8.2 VALUTAZIONE DEL RISCHIO RESIDUO 17
5.8.3 PIANO DI TRATTAMENTO DEL RISCHIO 17
5.8.4 IDENTIFICAZIONE DELLE AZIONI 17
5.8.5 PIANO DELLE AZIONI 17
5.9 APPROVAZIONE E ACCETTAZIONE DEL RISCHIO 18
5.10 MONITORAGGIO E REPORTING DEL RISCHIO 18
5.11 RIESAME 18
6 PRESIDI INTEGRATIVI PER IL COMUNE DI PARMA 19
6.1 CONTESTO, LEADERSHIP E RESPONSABILITÀ 19
6.2 APPROCCIO MULTI-RISCHIO E CRITERI DI ANALISI 19
6.3 CONTROLLI ISO/IEC 27001:2022 E DICHIARAZIONE DI APPLICABILITÀ 20
6.4 TRATTAMENTO, ECCEZIONI E AZIONI CORRETTIVE 20
6.5 VALUTAZIONE DELL'EFFICACIA, REPORTING E MIGLIORAMENTO 20

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.

La valutazione del rischio costituisce un elemento fondamentale per assicurare che i rischi che possono incidere sulle informazioni, sui sistemi, sui servizi digitali e sulla continuità dei servizi istituzionali siano identificati, analizzati, valutati, trattati, monitorati e riesaminati secondo criteri definiti e documentati.
IT.CITY S.p.A. supporta operativamente il processo.
La valutazione del rischio viene integrata dalla Procedura PR-SGSI-001 – Valutazione e Trattamento del rischio nell'ambito del SGSI di IT.CITY S.P.A.

Il presente documento è adottato in attuazione della misura ID.RA-05 prevista dall'Allegato 1 della Determinazione ACN n. 164179/2025. Il presente documento è approvato dagli organi di amministrazione e direttivi del Comune di Parma.

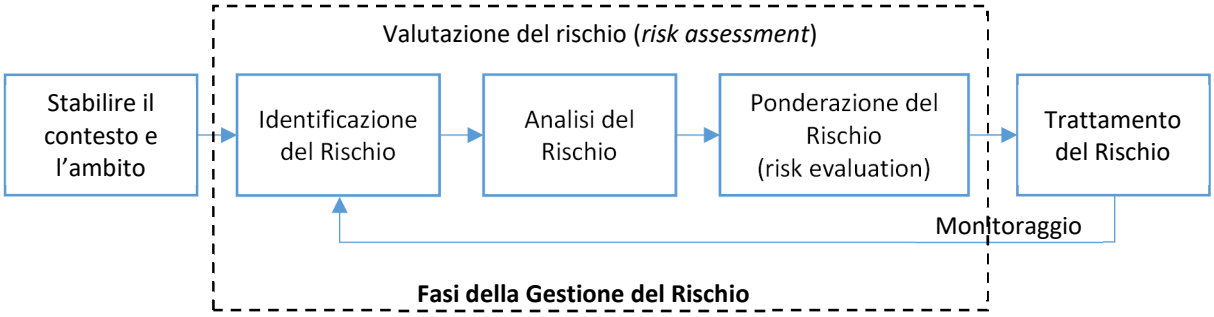
2 SCOPO E CAMPO DI APPLICAZIONE

Il presente documento disciplina il processo di valutazione e trattamento dei rischi per la sicurezza delle informazioni del Comune di Parma e definisce la metodologia, i criteri e le modalità adottati per l'identificazione, l'analisi, la ponderazione, il trattamento e il monitoraggio dei rischi.
A tal fine, il Comune di Parma assume quale riferimento metodologico la procedura PR-SGSI-001 definita nell'ambito del Sistema di Gestione per la Sicurezza delle Informazioni (SGSI) di IT.CITY S.p.A., applicandola e contestualizzandola alle caratteristiche, ai processi, ai servizi e alle responsabilità proprie dell'Ente.
Il processo si applica ai rischi derivanti da minacce e vulnerabilità che possono compromettere la riservatezza, l'integrità e la disponibilità delle informazioni (RID) e, ove pertinente, l'autenticità delle stesse, nonché la sicurezza e la continuità dei sistemi e dei servizi dell'Ente.
Il perimetro di applicazione comprende i processi e i servizi dell'Ente, le informazioni e i dati trattati, i sistemi informativi, le infrastrutture tecnologiche e fisiche, nonché le dipendenze da IT.CITY S.p.A., dai fornitori e dalle altre terze parti rilevanti. L'affidamento a IT.CITY S.p.A. o ad altri soggetti di attività operative non comporta il trasferimento delle responsabilità di governo, approvazione, supervisione e accettazione del rischio, che restano in capo al Comune di Parma secondo il proprio modello organizzativo.
La metodologia definisce i criteri per la determinazione del livello di rischio attraverso l'analisi degli asset, delle minacce, delle vulnerabilità e dei controlli di sicurezza esistenti. L'attribuzione dei valori è effettuata secondo criteri definiti e documentati, al fine di garantire, per quanto possibile, oggettività, coerenza e ripetibilità della valutazione a parità di contesto.

Le motivazioni alla base dei valori attribuiti sono documentate, in modo da assicurare la tracciabilità del processo di valutazione e consentire, in occasione dei successivi riesami, di verificare le variazioni intervenute nel contesto, nelle minacce, nelle vulnerabilità e nell'efficacia delle misure di sicurezza.
Per l'attribuzione dei valori agli asset, alle minacce e alle vulnerabilità si fa riferimento ai criteri e alle scale di valutazione definiti nel foglio di calcolo PR-SGSI001-A1, previsto nell'ambito del SGSI di IT.CITY S.p.A. e utilizzato, per quanto applicabile, per la valutazione dei rischi riferiti al perimetro del Comune di Parma.
Ai fini della presente procedura, il processo di risk assessment si articola nelle seguenti fasi:

1. Identificazione del rischio: individuazione degli scenari di rischio attraverso l'identificazione degli asset, delle minacce, delle vulnerabilità e dei controlli di sicurezza rilevanti;
2. Analisi del rischio: determinazione del livello di rischio sulla base dei criteri e dei parametri definiti dalla metodologia;
3. Ponderazione del rischio: confronto del livello di rischio con i criteri e le soglie di accettabilità definiti, al fine di stabilire se il rischio possa essere accettato oppure debba essere sottoposto a trattamento.

I rischi che richiedono un intervento sono sottoposti al successivo processo di trattamento, mediante l'individuazione delle misure necessarie alla loro riduzione, mitigazione, trasferimento o gestione. A seguito dell'attuazione delle misure, viene determinato il rischio residuo, che è sottoposto a valutazione e, ove ricorrano le condizioni previste, ad accettazione formale da parte dei soggetti competenti del Comune di Parma.



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
- Determinazione ACN n. 164179 del 14 aprile 2025 - Allegato 1 "Misure di sicurezza di base per i soggetti importanti"
- 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.
- Framework documentale specifico Comune di Parma
- Framework documentale IT.CITY S.P.A. Sistema di Gestione della Sicurezza delle Informazioni (SGSI)

- ISO 31000:2018 - Risk Management Principles and Guidelines

4 RUOLI E RESPONSABILITA'

All'interno del processo della valutazione del rischio vi sono diversi ruoli chiave che sono fondamentali nell'assicurare che tutti i rischi siano identificati, indirizzati e gestiti. Nella matrice RACI a seguire vengono indicati ruoli e rispettive responsabilità in ogni fase del processo di valutazione del rischio che verrà di seguito descritto.

R = Responsible A = Approvatore C = Consultato I = Informato

Ruolo / Step	RTD	Dirigenti	Organi di Amministrazione e Direttivi
Definizione del contesto	R	C	I
Identificazione dei rischi	C	R	I
Analisi dei rischi	C	R	I
Valutazione dei rischi	C	R	I
Trattamento del rischio	R	C	I
Approvazione dei rischi residui	C	C	A/R
Monitoraggio e reporting	R	I	A
Riesame	R	C	A

5 PROCESSO DI VALUTAZIONE E TRATTAMENTO DEL RISCHIO

Il processo di valutazione del rischio e del relativo trattamento è descritto più dettagliatamente nei seguenti sottoparagrafi.
I valori da assegnare ai livelli di rischio dipendono dalla scelta del metodo di calcolo. Vi sono due tipologie di metodi: quantitativi e qualitativi.

Metodi quantitativi

Nei metodi quantitativi si utilizza la seguente formula:

$$r(m, a, c) = p(m, c) * i(m, a, c)$$

dove:

- **m** = minaccia
- **a** = asset
- **c** = contesto / condizioni
- **p(m, c)** = probabilità (o frequenza annua) che la **minaccia m** si verifichi nel **contesto c**
- **i(m, a, c)** = perdita economica (€, k€) attesa se la **minaccia m** colpisce l'**asset a** nel **contesto c**
- **r(m, a, c)** = perdita annua attesa = *costo del rischio* (in € / anno, tipicamente)

Ovvero il **rischio** della combinazione minaccia – asset – contesto si calcola come:

Rischio atteso = **Probabilità che la minaccia si realizzi in quel contesto** * **Impatto economico se si realizza su quell'asset, in quel contesto**

Questo è un tipico modello **quantitativo** perché:
- **p** è una quantità reale (o frequenza)
- **i** è un importo economico

Vengono utilizzate in questo metodo la probabilità statistica o la frequenza delle minacce per determinare p(m, c) e la valutazione economica dei danni per determinare i(m, a, c).
I metodi quantitativi sono molto apprezzati nella teoria perché ritenuti precisi e oggettivi.
Nella pratica, quando si parla di sicurezza delle informazioni, non si hanno dati statistici affidabili sulle minacce e sugli attacchi e quindi questi metodi non garantiscono la precisione desiderata.
A questo bisogna aggiungere che l'analisi del rischio serve per fare ipotesi sul futuro, necessariamente soggettive e per le quali non possono esistere dati precisi. In altre parole, si può solo identificare il rischio percepito, ma quali mai quello reale.
Diventa quindi importante prestare attenzione al falso senso di oggettività delle metodologie quantitative: la mancanza di dati previsi ed affidabili (quando non la totale mancanza di dati) potrebbe far ritenere validi dati ottimistici e creare di conseguenza un falso senso di sicurezza.

Metodi qualitativi
I metodi qualitativi utilizzano delle scale di valori quali "Alto", "Medio" e "Basso" e applicano la seguente formula:

$$r(m, a, v) = p(m) * i(m, a) * g(v)$$

dove:
- **m** = minaccia
- **a** = asset
- **v** = vulnerabilità
- **p(m)** = **probabilità** della **minaccia m**
- **i(m, a)** = **impatto** della **minaccia m** sull'**asset a**
- **g(v) = gravità** della **vulnerabilità v** coinvolta
- **r(m, a, v) =** livello di rischio associato alla combinazione m, a, v

Esistono anche metodologie semi-quantitative, ma in realtà si tratta di metodologie qualitative che utilizzano valori quantitativi come linee guida per l'assegnazione dei valori. Questo approccio presenta gli stessi problemi delle metodologie quantitative: indisponibilità dei dati affidabili e falsa presunzione di oggettività.

Il processo adottato nella presente procedura è di tipo qualitativo, in quanto usa i termini Alto, Medio e Basso per descrivere il livello relativo di classificazione per ogni rischio specifico.

5.1 CRITERI PER L'ESECUZIONE DELLA VALUTAZIONE DEL RISCHIO

La valutazione del rischio è effettuata e aggiornata, in particolare:

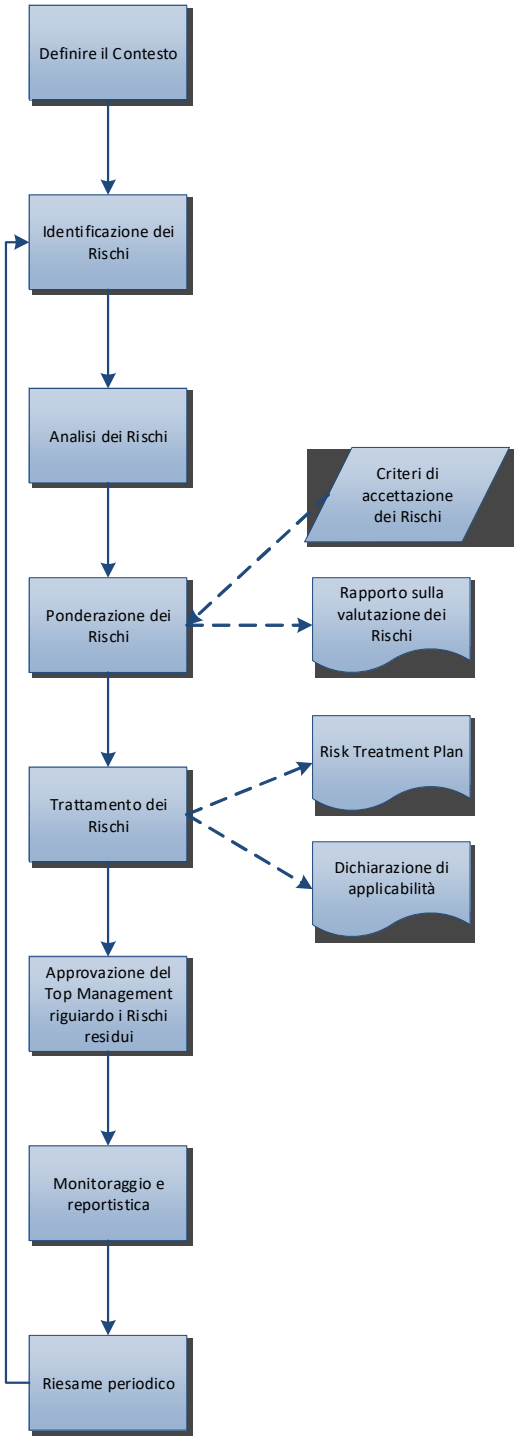
- nell'ambito della valutazione complessiva dei rischi del perimetro comunale;
- in occasione del riesame periodico del modello di gestione della sicurezza;
- in presenza di variazioni significative relative a processi, servizi, informazioni, sistemi o infrastrutture;
- nell'ambito di progetti che introducono modifiche significative al contesto tecnologico od organizzativo;
- nell'ambito dei processi di change management, ove il cambiamento possa incidere sul livello di rischio;
- in presenza di rilevanti modifiche normative, organizzative o del contesto di minaccia;
- nell'ambito della valutazione e selezione di fornitori, in particolare per servizi ICT e cloud.

5.2 CRITERI DI ACCETTAZIONE DEL RISCHIO

I criteri di accettazione del rischio sono definiti tenendo conto del contesto istituzionale del Comune di Parma, degli obblighi normativi e regolamentari applicabili, della criticità dei servizi, degli impatti potenziali, delle risorse disponibili e delle esigenze di continuità e resilienza dell'Ente.
L'accettazione del rischio costituisce una decisione consapevole e formalizzata.
L'eventuale accettazione del rischio residuo deve essere adeguatamente motivata, documentata, sottoposta a riesame e, ove opportuno, accompagnata da misure compensative o da specifiche attività di monitoraggio.

5.3 FLUSSO DEL PROCESSO DI VALUTAZIONE E TRATTAMENTO DEI RISCHI

Viene di seguito rappresentato il flusso del processo di valutazione e trattamento dei rischi e nei paragrafi a seguire ne vengono descritte le singole fasi.



5.4 DETERMINAZIONE DEL CONTESTO

Il contesto interno può includere:

- Governance, struttura organizzativa, ruoli e responsabilità
- Politiche, obiettivi, e strategie in essere per raggiungere gli obiettivi
- Capacità in termini di risorse e conoscenza (capitale, tempo, persone, processi, sistemi, tecnologie)

- Sistemi informativi, flussi di informazioni e processi decisionali (sia convenzionali che informali)
- Stakeholder interni: relazioni, percezioni e valori
- Cultura dell'organizzazione
- Norme, linee guida e modelli adottati dall'organizzazione
- Caratteristiche delle relazioni contrattuali
- Eventuale tipologia di servizi Cloud forniti

Il contesto esterno può includere:

- L'ambiente culturale, sociale, politico, legale, regolatore, finanziario, tecnologico, economico, naturale e competitivo: se internazionale, nazionale, regionale o locale
- Caratteristiche e trend che hanno impatto sugli obiettivi dell'organizzazione
- Stakeholder esterni: relazioni, percezioni e valori
- Standard settoriale riguardante la sicurezza dei fornitori di servizi Cloud – questo può essere affetto da tutti i recenti attacchi che hanno generato la perdita di integrità/disponibilità o confidenzialità di informazioni personalmente identificabili (PII)

Ambito e perimetro della valutazione del rischio sono definiti nei seguenti termini:

- Posizione geografica: per esempio regioni, uffici, Data Center
- Unità organizzative, per esempio specifici dipartimenti
- Processi dell'Ente
- Servizi, sistemi e reti IT
- soggetti destinatari dei servizi.

5.5 IDENTIFICAZIONE DEI RISCHI

Il processo di identificazione dei rischi riconducibili alla riservatezza, all'integrità o alla disponibilità delle informazioni richiede l'identificazione di:

- Asset
- Minacce
- Vulnerabilità e controlli di sicurezza
- Relazioni tra asset, minacce e vulnerabilità

5.5.1 Identificazione degli asset

I primi asset da identificare sono le informazioni per poi correlarle a tutti gli asset che le contengono o le trattano, inclusi quelli gestiti da fornitori.
Dopo aver individuato le informazioni, è necessario individuare gli altri asset utilizzati per trattarle o conservarle. Non si elencherà ogni singolo asset, ma si identificheranno delle loro aggregazioni basate su:

- omogeneità geografica per gli asset fisici;
- uso di procedure omogenee per la loro gestione;
- le persone responsabili degli asset.

L'inventario degli asset rilevanti del Comune di Parma è mantenuto attraverso le informazioni disponibili presso l'Ente e, per gli asset e i servizi affidati, attraverso gli strumenti e le evidenze gestiti da IT.CITY S.p.A.

5.5.2 Identificazione delle possibili minacce

Per ogni bene (o gruppo di beni) sono identificate le minacce che potrebbero ragionevolmente interferire. Queste varieranno secondo il tipo di bene e potrebbero essere eventi accidentali, quali ad esempio incendi o inondazioni, oppure attacchi dolosi, quali virus, furti o sabotaggi.
Le minacce si applicheranno ad uno o più caratteristiche fondamentali della sicurezza delle informazioni: la riservatezza, l'integrità e la disponibilità.

Le minacce sono classificate in agenti di minaccia, ossia sull'entità responsabile del manifestarsi della minaccia. Gli agenti di minaccia possono essere:

- persone malintenzionate (persone esterne o interne all'organizzazione)
- persone non malintenzionate (errori commessi da personale interno o esterno all'organizzazione)
- strumenti tecnici (possono manifestare comportamenti imprevisti dovuti alla loro scorretta progettazione o produzione, oppure per cause naturali quali per esempio polvere, temperature estreme o obsolescenza)
- natura (terremoti, inondazioni, ecc.)

5.5.3 Valutazione delle vulnerabilità e dei controlli di sicurezza in essere

Gli attributi di un bene (o del gruppo di beni) che possono essere sfruttati da una specifica minaccia saranno trattati come vulnerabilità e saranno dettagliati come componente della valutazione del rischio.
Esempi di tali vulnerabilità possono comprendere una mancanza di patch sui server (che potrebbe essere sfruttata dal Malware) o l'esistenza di archivi cartacei in un centro dati (che potrebbe andare distrutto in un incendio).
In questa fase viene elaborata una lista di vulnerabilità o controlli di sicurezza, in modo da renderne sistematica l'identificazione e la valutazione. Sono utilizzati i controlli di sicurezza della ISO/IEC 27002:2022.

5.5.4 Identificazione degli scenari di rischio

L'identificazione dei rischi per la sicurezza delle informazioni dell'organizzazione è realizzata tramite una combinazione di riunioni e di interviste di gruppo con le parti interessate.
Tali parti interessate includono normalmente (quando possibile):

- Responsabili dei processi, dei servizi e delle attività critiche dell'Ente;
- referenti organizzativi e tecnici dei processi e dei servizi interessati;
- Chi gestisce l'input/output dell'attività
- Parti terze con conoscenze particolari
- Rappresentanti di chi fornisce i servizi e le risorse di sostegno all'attività
- Qualunque altra parte che può fornire informazioni utili al processo di identificazione dei rischi

5.6 ANALISI DEL RISCHIO

Il metodo di analisi adottato è di tipo qualitativo e utilizza scale numeriche ordinali come supporto all'attribuzione dei livelli di rischio Basso, Medio e Alto. I valori numerici non rappresentano una quantificazione economica del rischio, ma costituiscono un supporto alla classificazione e alla comparabilità delle valutazioni.

Vengono assegnati valori agli asset, alle minacce e alle vulnerabilità (o controlli di sicurezza). Tali valori sono per quanto possibile oggettivi e ripetibili. All'interno del foglio di calcolo VERA sono indicate le linee guida per l'attribuzione dei valori.
Il metodo di analisi è qualitativo e utilizza scale di valori quali Alto-Medio-Basso.

5.6.1 Criteri di valutazione delle informazioni

Con il metodo VERA vengono valutate le informazioni ed il potenziale danno dovuto alla perdita di riservatezza, integrità e disponibilità, assegnando un valore da 1 (Basso) a 4 (Critico) secondo le linee guida riportate nella tabella a seguire.

Livello	R – Riservatezza	I – Integrità	D – Disponibilità
1 – Basso	I dati non presentano particolari requisiti di riservatezza. I dati sono pubblici.	I dati non presentano particolari requisiti di integrità. I dati gestiti non fanno parte di transazioni economiche, finanziarie o sanitarie.	L'indisponibilità dei dati oltre i tempi stabiliti contrattualmente non comporta multe o penali rilevanti.
2 – Medio	I dati devono essere riservati per ragioni di business (concorrenza sleale, danni all'immagine), ma un'eventuale loro diffusione non ha elevati impatti sul business dell'organizzazione, sul rispetto della normativa vigente o sull'immagine dell'organizzazione.	I dati non sono oggetto di transazioni di tipo economico, finanziario o sanitario con impatti sul business di un'impresa. La mancanza di integrità dei dati non ha elevati impatti sulle attività operative o sul rispetto della normativa vigente.	L'indisponibilità dei dati oltre i tempi stabiliti contrattualmente comporta multe o penali non particolarmente rilevanti.
3 – Alto	I dati devono essere riservati per ragioni di business (concorrenza sleale, danni all'immagine), ma un'eventuale loro diffusione non ha elevati impatti sul business dell'organizzazione, sul rispetto della normativa vigente o sull'immagine dell'organizzazione.	I dati non sono oggetto di transazioni di tipo economico, finanziario o sanitarie con impatti sul business di un'impresa. La mancanza di integrità dei dati non ha elevati impatti sulle attività operative o sul rispetto della normativa vigente.	L'indisponibilità dei dati oltre i tempi stabiliti contrattualmente comporta multe o penali rilevanti.
4 – Critico	La diffusione delle informazioni ha elevati impatti sul business dell'organizzazione o sul rispetto della normativa vigente o sull'immagine dell'organizzazione tali da compromettere la sostenibilità dell'organizzazione.	La mancanza di integrità delle informazioni ha elevati impatti sul business aziendale o sul rispetto della normativa vigente tali da compromettere la sostenibilità dell'organizzazione.	L'indisponibilità dei dati oltre i tempi stabiliti contrattualmente comporta multe o penali che mettono in pericolo la sostenibilità economica e di immagine o hanno impatti sulla sicurezza delle persone fisiche.

5.6.2 Identificazione e valutazione delle minacce

Vengono identificate le possibili minacce, e viene valutato il loro grado di verosimiglianza. Per svolgere questa attività, in generale, si considera se tale evento è già accaduto nell'organizzazione in esame, oppure in organizzazioni simili, e si stabilisce se esistano motivazioni, opportunità e capacità sufficienti affinché una determinata minaccia si concretizzi. Nell'ambito del metodo VERA, alla verosimiglianza delle minacce è assegnato un valore su una scala da 1 (Bassa) a 3 (Alta), secondo i criteri riportati nella tabella seguente.

Livello	Linee guida per la verosimiglianza
1 – Bassa	È applicabile ad almeno uno dei seguenti casi: - la minaccia si può verificare con frequenza inferiore rispetto a quanto riportato dalle ricerche più note; - in caso di **attacco deliberato**, i dati sono poco appetibili e l'immagine aziendale non è compromessa e pertanto i tentativi di attacco o non sono iniziati o sono condotti da malintenzionati scarsamente preparati da un punto di vista tecnico, e con scarse risorse a disposizione; - in caso di attacco **non deliberato**, l'ambito è poco complesso e quindi è difficile commettere errori; - in caso di **eventi naturali**, gli studi dimostrano che la minaccia può verificarsi molto raramente.
2 – Media	È applicabile ad almeno uno dei seguenti casi: - la minaccia si può verificare secondo quanto riportato dalle ricerche più note; - in caso di **attacco deliberato**, i dati sono poco appetibili e l'immagine aziendale non è compromessa e quindi può essere condotto da malintenzionati non particolarmente motivati, mediamente preparati da un punto di vista tecnico e con scarse risorse a disposizione; in alternativa, gli studi confermano che i tentativi di attacco sono comunque rari; - in caso di **attacco non deliberato**, l'ambito è mediamente complesso e quindi possono essere commessi errori; - in caso di **eventi naturali**, gli studi dimostrano che la minaccia può verificarsi nella media dei casi studiati.
3 – Alta	È applicabile ad almeno uno dei seguenti casi: - la minaccia si può verificare più frequentemente rispetto a quanto riportato dalle ricerche più note; - in caso di **attacco deliberato**, i dati sono appetibili o l'immagine aziendale è compromessa, e quindi può essere condotto da malintenzionati molto motivati, tecnicamente preparati e con ingenti risorse a disposizione; in alternativa, gli studi confermano che tentativi di attacco sono comunque portati molto di frequente; - in caso di attacco **non deliberato**, l'ambito è di elevata complessità (per esempio per molteplicità di sedi, tipologie di sistemi informatici, utenti interni e/o esterni) e quindi è facile siano commessi errori; - in caso di **eventi naturali**, gli studi dimostrano che la minaccia si verifica quasi certamente.

5.6.3 Valutazione efficacia dei controlli della ISO/IEC 27001:2022

Viene successivamente valutata l'efficacia dei vari controlli di sicurezza attivi (quando applicabili dall'organizzazione), utilizzando la lista ISO/IEC 27001:2022 e secondo la tabella che segue.

Livello	Linee guida per la valutazione

1 – Inadeguato	Il controllo non è previsto o è assente nella pratica.
2 – Parzialmente adeguato	Il controllo è applicato sporadicamente o in modo completamente inadeguato, non garantendone quindi l'efficacia.
3 – Quasi adeguato	Sono state rilevate mancanze al controllo, soprattutto di tipo formale (per esempio, inesattezze nelle procedure relative).
4 – Adeguato	Il controllo è sistematicamente applicato e non sono state rilevate inadeguatezze al controllo.

I controlli attuati per ciascun asset vengono confrontati con quelli ideali, in modo da attribuire un valore rispetto all'adeguatezza e conformità.
A titolo di semplice esempio, si supponga che il controllo ideale per importanti documenti di progettazione preveda l'utilizzo di una cassaforte. Nel caso non sia presente la cassaforte, il controllo risulterà assente quindi valorizzato 1 (Inadeguato). Nel caso fosse presente una cassaforte, ma venisse lasciata mediamente aperta, il controllo risulterebbe non conforme e dovrebbe essere valorizzato 2 (Parzialmente adeguato).

5.6.4 Classificazione del rischio

Per calcolare il livello di rischio si utilizzano formule di calcolo del rischio intrinseco (combinazione tra il valore degli asset e la probabilità di accadimento di una minaccia) aggiungendo il parametro di vulnerabilità. Per ogni minaccia, e per ogni controllo che può mitigarne la verosimiglianza o l'impatto, viene quindi calcolato un livello di rischio (vedi documento di calcolo VERA, foglio calcolo del rischio).
Ad ogni rischio è assegnato un livello in base al proprio punteggio, come di seguito indicato.

Controllo	Minaccia	Vulnerabilità
1	1	1
2	2	2
3	3	3

Livello di rischio
Basso < 20
19 < Medio < 41
Alto > 40

La classificazione di ogni rischio sarà registrata come input in fase di ponderazione del rischio.

5.7 PONDERAZIONE DEL RISCHIO

Lo scopo della ponderazione del rischio è di decidere quali rischi possono essere accettati e quali devono essere trattati. Ciò dovrebbe considerare i criteri di accettazione del rischio stabiliti per questa valutazione specifica (vedere i suddetti criteri di accettazione del rischio).
La tabella al paragrafo 5.6.4 mostra il criterio di classificazione del rischio, dove il verde indica che il rischio è sotto la soglia accettabile. Le aree in giallo e in rosso generalmente indicano che un rischio non risponde ai criteri di accettazione, ed è un candidato per il trattamento.

Per il trattamento, i rischi saranno ordinati per priorità secondo il loro punteggio e la loro classificazione, in modo da gestire con priorità i rischi con punteggio maggiore, e in ogni caso prima di trattare quelli con i livelli più bassi.

5.7.1 Report di valutazione del rischio

Il Report di valutazione del rischio costituisce l'output della fase di valutazione e l'input per il successivo trattamento. Gli esiti sono sottoposti ai soggetti competenti del Comune di Parma secondo le responsabilità definite nel modello organizzativo dell'Ente. Le decisioni relative all'accettazione dei rischi sono formalizzate e tracciate.

5.8 TRATTAMENTO DEL RISCHIO

Per i rischi riferiti al perimetro del Comune di Parma che risultano superiori alla soglia di accettabilità definita dall'Ente devono essere individuate e formalizzate le opportune modalità di trattamento. IT.CITY S.p.A. supporta la definizione e l'attuazione delle misure.
Scopo del trattamento di un rischio è di ridurre la classificazione dello stesso ad un livello almeno accettabile.

Nota 1: il trattamento può comportare le possibili seguenti opzioni:

- evitare il rischio decidendo di non iniziare o continuare un'attività;
- aumentare il rischio per cogliere un'opportunità;
- rimuovere la sorgente del rischio, ossia la minaccia;
- modificare la probabilità della minaccia;
- modificare le conseguenze dell'accadimento dannoso (per esempio effettuando i backup);
- condividere il rischio con altri soggetti (anche attraverso contratti e finanziamenti);
- mantenere il rischio con una scelta informata e consapevole.

Nota 2: i trattamenti relativi a conseguenze negative sono spesso indicati con le espressioni "mitigazione del rischio", "eliminazione del rischio", "prevenzione del rischio" e/o "riduzione del rischio".

Nota 3: il trattamento del rischio può creare nuovi rischi o modificare quelli esisteni.

A volte, nonostante si riduca il livello di rischio, il rischio potrebbe rimanere allo stesso livello di classificazione.
Qualora, a seguito dell'attuazione delle misure di trattamento, permanga un rischio residuo, la relativa accettazione è sottoposta ai soggetti competenti del Comune di Parma. La decisione deve essere motivata, formalizzata, limitata nel tempo, corredata dalle eventuali misure compensative e sottoposta a riesame periodico.

5.8.1 Opzioni di trattamento del rischio

Per il trattamento dei rischi che sono stati definiti inaccettabili si può scegliere di applicare una delle seguenti opzioni:

1. Modificare il rischio, ovvero ridurre la probabilità o l'impatto del rischio in maniera che risulti accettabile
2. Evitare il rischio attraverso una strategia per cui il rischio non è più accettabile
3. Condividere il rischio con un'altra parte (per esempio un'assicurazione oppure un fornitore)

La strategia da seguire sarà dettata di volta in volta dalle circostanze, dalla conoscenza delle problematiche e dalla conoscenza del contesto interno ed esterno

5.8.2 Valutazione del rischio residuo

A seguito dell'individuazione e dell'attuazione delle misure di trattamento, il rischio è nuovamente valutato al fine di determinarne il livello residuo. Il rischio residuo rappresenta il livello di rischio che permane tenendo conto delle misure di sicurezza esistenti e di quelle attuate nell'ambito del trattamento.
Il livello di rischio residuo è confrontato con i criteri e le soglie di accettabilità definiti per il perimetro del Comune di Parma. Qualora il rischio residuo risulti accettabile, la relativa accettazione è formalizzata dai soggetti competenti dell'Ente; qualora risulti superiore alla soglia di accettabilità, sono individuate ulteriori misure di trattamento oppure la decisione è sottoposta agli Organi competenti per le determinazioni del caso.
L'accettazione del rischio residuo deve essere motivata, documentata, limitata nel tempo e sottoposta a riesame periodico, anche in relazione a variazioni del contesto, delle minacce, delle vulnerabilità o dell'efficacia delle misure adottate.

5.8.3 Piano di trattamento del rischio

L'insieme di tutte le decisioni prese, rischio per rischio, determina il Piano di trattamento del rischio (Risk treatment plan).

5.8.4 Identificazione delle azioni

Prima di stabilire definitivamente se ridurre o meno un rischio vengono identificate le azioni necessarie e per ciascuna di essere i benefici attesi.
L'elenco delle azioni previste viene riesaminato per accertarsi che queste siano tra loro coerenti, fattibili e non introducano nuovi rischi inaccettabili. Infine, le azioni vengono pianificate in dettaglio e monitorate fino alla conclusione e alla valutazione della loro efficacia.
Per valutare se un'azione possa portare ad una riduzione del rischio viene effettuata una "what-if analisys", vale a dire la determinazione dei valori previsti per asset, minacce e vulnerabilità a seguito della conclusione dell'azione, in modo da calcolare il livello di rischio che si otterrebbe.

5.8.5 Piano delle azioni

Dopo aver scelto le azioni da intraprendere e pesati i benefici attesi, le azioni vengono pianificate coinvolgendo le parti interessate e predisponendo un registro delle azioni di miglioramento, contenente:

- rischi che richiedono trattamento;
- risorse necessarie
- azioni da implementare;
- persone responsabili delle azioni da implementare;
- cronoprogramma delle azioni da implementare e relative scadenze;
- livelli di rischio residuo dopo che i controlli sono stati implementati;
- modalità in cui verrà valutata l'efficacia.

5.9 APPROVAZIONE E ACCETTAZIONE DEL RISCHIO

Gli Organi e le funzioni competenti del Comune di Parma sono informati sugli esiti della valutazione dei rischi, sulle decisioni di trattamento e sul rischio residuo, secondo le responsabilità definite nel modello organizzativo dell'Ente.
Il Piano di trattamento del rischio è sottoposto all'approvazione degli Organi di amministrazione e direttivi competenti. L'accettazione dei rischi residui è formalizzata dai soggetti competenti secondo le soglie e le modalità definite dall'Ente.

5.10 MONITORAGGIO E REPORTING DEL RISCHIO

Come parte dell'implementazione di nuovi controlli e della manutenzione di quelli in essere, verranno identificati e definiti gli indicatori chiave che permetteranno di misurare il raggiungimento degli obiettivi riguardanti il controllo del rischio.
Questi indicatori saranno stilati regolarmente, così come il trend, in maniera da poter identificare e trattare situazioni anomale.
Il monitoraggio costituisce parte integrante del modello di gestione della sicurezza del Comune di Parma e, per gli ambiti di competenza, dei processi operativi previsti dal SGSI di IT.CITY S.p.A.

5.11 RIESAME

La valutazione del rischio è sottoposta a riesame almeno annualmente e ogniqualvolta intervengano variazioni significative del contesto normativo, organizzativo o tecnologico, modifiche del perimetro, introduzione o variazione di servizi e sistemi, cambiamenti rilevanti relativi ai fornitori, incidenti significativi, vulnerabilità critiche o variazioni dell'esposizione alle minacce. Il riesame verifica inoltre che le misure esistenti mantengano nel tempo un livello di efficacia adeguato.

6 PRESIDI ORGANIZZATIVI E DI CONTROLLO

6.1 CONTESTO, LEADERSHIP E RESPONSABILITÀ

La valutazione e il trattamento dei rischi costituiscono una componente fondamentale del modello organizzativo del Comune di Parma per la sicurezza delle informazioni e la cybersicurezza. Il processo è svolto tenendo conto dei principi e dei criteri della ISO/IEC 27001:2022 e della ISO/IEC 27005:2022 e, per gli aspetti operativi e metodologici, integra le procedure e gli strumenti del SGSI di IT.CITY S.p.A. applicabili al perimetro comunale.
Gli Organi di amministrazione e direttivi competenti approvano il Piano di trattamento del rischio. Il Responsabile per la Transizione Digitale coordina il processo per il Comune di Parma, assicura la tracciabilità delle decisioni e acquisisce da IT.CITY S.p.A., dai responsabili degli asset, dalle strutture comunali e dagli altri soggetti coinvolti le informazioni e le evidenze necessarie. Le competenze e le soglie approvative sono definite nel documento "Organizzazione per la sicurezza informatica – Ruoli e responsabilità".

6.2 APPROCCIO MULTI-RISCHIO E CRITERI DI ANALISI

In attuazione dell'art. 24 del D.Lgs. 138/2024, la valutazione adotta un approccio multi-rischio e considera eventi cyber, tecnologici, fisici, ambientali, organizzativi e di terza parte. Gli scenari comprendono almeno indisponibilità o degrado dei servizi, compromissione di riservatezza, integrità, autenticità o tracciabilità, danni a persone fisiche o giuridiche, perdite materiali o immateriali, impatti economici, normativi e reputazionali e possibili effetti su altri servizi o amministrazioni.
L'approccio multi-rischio prevede l'adozione dei seguenti criteri:

- sicurezza della catena di approvvigionamento, incluse vulnerabilità dei fornitori diretti, subfornitori, prodotti e servizi ICT e processi di sviluppo sicuro;
- sicurezza dei servizi cloud, secondo il modello di responsabilità condivisa che include localizzazione e portabilità dei dati, continuità, dipendenza dal fornitore, gestione delle identità, logging, cifratura e strategia di uscita;
- acquisizione, sviluppo e manutenzione sicura dei sistemi, incluse gestione delle vulnerabilità, configurazioni, componenti software e, ove applicabile, codifica sicura;
- continuità operativa, backup, disaster recovery, gestione delle crisi e prontezza ICT, con riferimento a RTO, RPO, dipendenze e capacità di ripristino;
- sicurezza e affidabilità del personale, controllo degli accessi, MFA, gestione degli asset, crittografia e comunicazioni protette;
- monitoraggio degli accessi e delle aree che ospitano informazioni o infrastrutture rilevanti.

La probabilità è supportata da informazioni di threat intelligence aggiornate, bollettini ACN/CSIRT Italia, avvisi dei produttori e dei fornitori, evidenze SOC, incidenti interni ed esterni, vulnerabilità note e cambiamenti del contesto. Le fonti, la data di acquisizione e le motivazioni dei valori assegnati sono registrate per garantire ripetibilità e riesame.

6.3 CONTROLLI ISO/IEC 27001:2022 E DICHIARAZIONE DI APPLICABILITÀ

La selezione e la valutazione dei controlli considerano l'intero Annex A e, in particolare, i controlli introdotti o rafforzati nell'edizione 2022. Per ciascun controllo sono indicati applicabilità, motivazione, responsabile, stato di attuazione, evidenze, rischi trattati e collegamento alle misure NIS2.

- A.5.7 Threat intelligence: raccolta, analisi, contestualizzazione e utilizzo operativo delle informazioni sulle minacce;
- A.5.23 Sicurezza delle informazioni per l'uso di servizi cloud: requisiti lungo acquisizione, utilizzo, gestione e cessazione del servizio;
- A.5.30 Prontezza ICT per la continuità operativa: capacità ICT coerenti con BIA, RTO/RPO, test e piani BC/DR;
- A.7.4 Monitoraggio della sicurezza fisica: sorveglianza proporzionata al rischio delle aree e delle infrastrutture;
- A.8.9 Gestione della configurazione: baseline sicure, inventario, controllo delle modifiche e verifica delle deviazioni;
- A.8.10 Cancellazione delle informazioni: cancellazione sicura e verificabile al termine del periodo di conservazione o del rapporto contrattuale;
- A.8.11 Data masking: mascheramento o pseudonimizzazione dei dati quando richiesto dal rischio e dalla finalità;
- A.8.12 Prevenzione della perdita di dati: misure DLP organizzative e tecniche sui canali e sugli asset rilevanti;
- A.8.16 Attività di monitoraggio: logging, correlazione, SOC e rilevazione di comportamenti anomali;
- A.8.23 Web filtering: controllo dell'accesso a risorse web malevole o non autorizzate;
- A.8.28 Codifica sicura: principi, verifiche e requisiti contrattuali per sviluppi interni o affidati a fornitori, ove applicabile.

6.4 TRATTAMENTO, ECCEZIONI E AZIONI CORRETTIVE

La valutazione dei rischi e il Piano di Trattamento/Adeguamento riportano almeno: servizio e processo interessato, asset e proprietario, scenario e fonte, impatti, probabilità, rischio intrinseco e residuo, controlli esistenti e pianificati, responsabile, risorse, scadenza, indicatori di efficacia, evidenze, dipendenze da fornitori e data del riesame.

L'accettazione del rischio residuo è motivata, formalizzata, limitata nel tempo e soggetta a riesame. I rischi elevati, le eccezioni ai requisiti obbligatori e le azioni scadute sono tempestivamente escalati al RTD e agli Organi competenti. Qualora emerga una non conformità rispetto alle misure di cui all'art. 24 del D.Lgs. 138/2024, sono avviate senza indebito ritardo misure correttive appropriate e proporzionate; l'eventuale impossibilità temporanea è accompagnata da misure compensative e da un termine approvato.

Le vulnerabilità tecniche sono trattate secondo il "Piano di Gestione delle Vulnerabilità"; i rischi di terza parte secondo "Audit e Monitoraggio Fornitori" e "Sicurezza Informatica Esterni"; gli interventi non immediatamente realizzabili confluiscono nel "Piano di Adeguamento".

6.5 VALUTAZIONE DELL'EFFICACIA, REPORTING E MIGLIORAMENTO

L'efficacia delle misure è valutata mediante indicatori, test, audit, vulnerability assessment, esercitazioni BC/DR, analisi degli incidenti, verifiche di configurazione e riesami delle evidenze. Il reporting evidenzia andamento del rischio, rischi elevati e scaduti, efficacia dei controlli, eccezioni, dipendenze critiche e decisioni richieste agli Organi di Amministrazione e Direttivi.

Il riesame è effettuato almeno annualmente e a seguito di incidenti significativi, variazioni organizzative o normative, introduzione di nuovi servizi o tecnologie, cambiamenti rilevanti relativi a fornitori o servizi cloud, vulnerabilità critiche, esiti di audit, evoluzione delle minacce o risultati non soddisfacenti delle verifiche. Le lezioni apprese alimentano il miglioramento continuo del modello di gestione della sicurezza del Comune di Parma e, per gli ambiti di competenza, del SGSI di IT.CITY S.p.A., nonché l'aggiornamento coordinato del Piano di trattamento del rischio e del Piano di adeguamento.