Comune di Parma

PIANO DI GESTIONE DELLE VULNERABILITA’

Documento per approvazione formale ai fini ID.RA-08

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' 6
5 STRATEGIA DI MONITORAGGIO DELLA SICUREZZA, DELLE RETI E DEI SISTEMI 6
5.1 IMPLEMENTAZIONE DEI SISTEMI DI MONITORAGGIO 7
5.2 EVENTI DA MONITORARE 7
5.3 ANALISI E NOTIFICA DEGLI EVENTI 7
5.4 ANALISI DELLE ANOMALIE E CORRELAZIONE (DE.CM-09) 8
6 STRATEGIA PER LA GESTIONE DELLE VULNERABILITA' TECNICHE 8
6.1 IDENTIFICAZIONE DELLE VULNERABILITA' 8
6.2 VALUTAZIONE DELLE VULNERABILITA' 8
6.3 TRATTAMENTO DELLE VULNERABILITA' 9
6.4 MONITORAGGIO E REVISIONE 9
6.5 THREAT INTELLIGENCE 9
6.6 DIVULGAZIONE COORDINATA DELLE VULNERABILITA' (CVD) (ART. 16 D.LGS. 138/2024) 9
7 FORMAZIONE E SENSIBILIZZAZIONE DEGLI UTENTI 9
8 MONITORAGGIO, KPI E MIGLIORAMENTO CONTINUO 10
9 DOCUMENTAZIONE E REPORTING 10
10 REVISIONE DELLA POLITICA 10
11 CONTATTI E SUPPORTO 10
12 PRESIDI INTEGRATIVI ISO/IEC 27001:2022 E NIS2 11
12.1 COLLEGAMENTO CON IL RISCHIO E LA DICHIARAZIONE DI APPLICABILITÀ 11
12.2 PERIMETRO, INVENTARIO E FONTI DI RILEVAZIONE 11
12.3 VALUTAZIONE E PRIORITIZZAZIONE BASATA SUL RISCHIO 11
12.4 REMEDIATION, CONFIGURAZIONE E SVILUPPO SICURO 11
12.5 CLOUD, FORNITORI E NOTIFICA A CASCATA 12
12.6 MONITORAGGIO, INCIDENTI E THREAT INTELLIGENCE 12
12.7 KPI, REPORTING, RIESAME E MIGLIORAMENTO 12

1 INTRODUZIONE

Il Comune di Parma adotta un proprio modello organizzativo e di governo per la gestione della sicurezza delle informazioni e della cybersicurezza, nell'ambito del quale sono definiti ruoli, responsabilità, autorità e funzioni di indirizzo, governo, supervisione e controllo.
Per l'attuazione operativa di tale modello, il Comune si avvale del Sistema di Gestione per la Sicurezza delle Informazioni (SGSI) adottato da IT.CITY S.p.A., società in house dell'Ente, nonché delle relative politiche, procedure, metodologie e misure di sicurezza, per quanto applicabili ai servizi affidati e al perimetro comunale.
Restano in capo al Comune di Parma la governance complessiva della sicurezza, l'indirizzo strategico, il governo e l'accettazione del rischio, l'approvazione delle misure e dei piani di propria competenza, la supervisione e la vigilanza sulla loro attuazione, in conformità al Decreto Legislativo 4 settembre 2024, n. 138 e alle altre disposizioni applicabili in materia di cybersicurezza.

Il presente Piano disciplina il modello adottato dal Comune di Parma per la gestione delle vulnerabilità nell'ambito del proprio sistema di governo della sicurezza delle informazioni. Per le attività operative relative ai sistemi e servizi affidati, il Comune si avvale di IT.CITY S.p.A., che opera secondo il proprio SGSI e, in particolare, secondo la Politica POL-SGSI-088 "Gestione delle vulnerabilità", per quanto applicabile al perimetro dei servizi gestiti. Restano in capo al Comune le funzioni di indirizzo, approvazione, supervisione, vigilanza e governo del rischio.

2 SCOPO E CAMPO DI APPLICAZIONE

Il presente documento definisce i principi, i processi e le responsabilità per il monitoraggio delle risorse ICT e per la gestione delle vulnerabilità dei sistemi, dei dispositivi, delle reti, delle applicazioni e delle ulteriori risorse informatiche utilizzate dal Comune di Parma, comprese quelle gestite da IT.CITY S.p.A. o da fornitori. Il processo comprende rilevazione, valutazione basata sul rischio, prioritizzazione, trattamento, verifica della remediation, threat intelligence, reporting e formazione, in coerenza con ISO/IEC 27001:2022, ISO/IEC 27002:2022, NIST CSF e D.Lgs. 138/2024.

Il Comune di Parma, in qualità di soggetto importante ai sensi del D.Lgs. 138/2024 (NIS2), adotta il presente Piano quale misura organizzativa e tecnica a supporto degli obblighi di governance e gestione del rischio. IT.CITY S.p.A. ne assicura l'attuazione operativa per i sistemi e i servizi gestiti, ferma restando la responsabilità del Comune in materia di indirizzo, approvazione, supervisione e vigilanza.

Questo documento risponde specificamente ai requisiti della Categoria DE.CM (Rilevamento) del Framework Nazionale di Cyber Security, in particolare:

- DE.CM-01: monitoraggio continuo dei sistemi e delle reti per rilevare eventi potenzialmente compromettenti.
- DE.CM-09: raccolta e analisi dei log per l'individuazione di anomalie. Inoltre, supporta l'adempimento degli obblighi di gestione e notifica degli incidenti (art. 25 del decreto).

Il documento definisce un approccio proattivo e strutturato per la gestione delle vulnerabilità, sostenendo la resilienza e la protezione delle informazioni.

Il Piano si applica al perimetro del Comune di Parma e ai sistemi e servizi gestiti da IT.CITY S.p.A., inclusi infrastrutture on-premise e cloud, endpoint, dispositivi mobili, apparati di rete e sicurezza, applicazioni, database, componenti software, codice e dipendenze, nonché asset gestiti da fornitori e terze parti che accedono a informazioni o sistemi dell'Ente.

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" (DE.CM-01, DE.CM-09)
- 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)
- NIST Cybersecurity Framework

4 RUOLI E RESPONSABILITA'

Gli Organi di Amministrazione e Direttivi del Comune di Parma approvano il Piano e ne sovrintendono l'attuazione. Ricevono reporting periodico e tempestivo sulle esposizioni critiche, garantiscono le risorse necessarie, verificano le eccezioni e promuovono la formazione in materia di sicurezza informatica.

Il Responsabile per la Transizione Digitale coordina il presidio per il Comune. Il Responsabile della Sicurezza delle Informazioni e il Team IT di IT.CITY S.p.A. assicurano, per i sistemi gestiti, le attività operative di monitoraggio, vulnerability assessment, patch management, escalation e reporting, in raccordo con i proprietari degli asset e dei servizi.

Il personale del Comune, di IT.CITY S.p.A. e dei fornitori coinvolti coopera alle attività di rilevazione e remediation, partecipa alla formazione applicabile e segnala tempestivamente anomalie e vulnerabilità secondo i canali definiti.

5 STRATEGIA DI MONITORAGGIO DELLA SICUREZZA, DELLE RETI E DEI SISTEMI

IT.CITY adotta attività di monitoraggio continuo degli eventi di sicurezza, mediante strumenti di logging, analisi dei log, threat intelligence e rilevazione delle anomalie, al fine di individuare tempestivamente eventi potenzialmente avversi.

5.1 IMPLEMENTAZIONE DEI SISTEMI DI MONITORAGGIO

Il perimetro di monitoraggio è definito sulla base dell'analisi dei rischi e della criticità degli asset per la continuità dei servizi essenziali del Comune di Parma. Le modalità operative per la configurazione delle sorgenti di log, la centralizzazione dei flussi, le misure tecniche a garanzia dell'integrità e i tempi specifici di conservazione (retention policy) sono definiti in dettaglio nella procedura operativa **PR-SGSI-011 "Gestione e Conservazione dei Log" (SGSI di IT.CITY)**, in conformità ai requisiti di forensic readiness richiesti dal D.Lgs 138/2024.
Sono soggetti a monitoraggio continuo (24/7 automatizzato):

- tutti i sistemi informatici e di rete rilevanti. I sistemi di autenticazione critica (Active Directory), i dispositivi di rete, i server, i sistemi operativi, i middleware e le applicazioni sono monitorati attraverso strumenti SIEM, IDS/IPS, e log management.
- i punti di interscambio con reti pubbliche (firewall perimetrali)
- gli endpoint gestiti (tramite EDR/XDR)
- i log raccolti da:
  - firewall e dispositivi perimetrali,
  - endpoint,
  - server applicativi e database,
  - sistemi di autenticazione e autorizzazione

  e collezionati centralmente in soluzioni di auditing e/o SOC.

5.2 EVENTI DA MONITORARE

- Accessi non autorizzati o tentativi di accesso
- Modifiche e trasferimenti anomali e/o non autorizzati di dati
- Elevazione di privilegi non prevista
- Comunicazioni di rete inusuali o verso destinazioni non autorizzate
- Esecuzione di software non autorizzato

5.3 ANALISI E NOTIFICA DEGLI EVENTI

- Gli eventi critici vengono correlati e analizzati automaticamente da soluzioni di auditing e MDR.
- In caso di rilevazione di un evento classificabile come “potenzialmente avverso”, viene generato un alert per il team di sicurezza (interno ed esterno).
- Tutti gli eventi vengono documentati e archiviati per almeno 24 mesi per scopi di audit e investigazione dell’auditor.
- Qualora l’evento rilevato presenti le caratteristiche di un incidente significativo ai sensi dell’art. 25 del D.Lgs. 138/2024, il Team IT e il Referente CSIRT attivano immediatamente la Procedura di Gestione degli Incidenti. La procedura assicura la pre-notifica al CSIRT Italia entro 24 ore dalla conoscenza, la notifica entro 72 ore, gli eventuali aggiornamenti richiesti e la relazione finale entro un mese dalla notifica, secondo i criteri e le modalità applicabili.
- Al fine di garantire la validità legale delle registrazioni in caso di incidente (art. 25 D.Lgs. 138/2024) o indagine giudiziaria, i log sono gestiti garantendone inalterabilità e disponibilità secondo il ciclo di vita descritto nella **PR-SGSI-011 (SGSI di IT.CITY)**. Tale procedura assicura che nessuna evidenza possa essere cancellata o modificata dagli amministratori di sistema al di fuori delle finestre di retention approvate.

Sono definiti livelli di logging per ogni tipo di sistema.
I log includono: timestamp, identità utente, indirizzo IP, evento eseguito, esito.

I file di log sono protetti da accessi non autorizzati e archiviati in modo sicuro per garantirne l'integrità in soluzione di backup offline.

5.4 ANALISI DELLE ANOMALIE E CORRELAZIONE (DE.CM-09)

Oltre al rilevamento basato su firme (signature.based) per minacce note, IT.CITY implementa meccanismi di analisi comportamentale per identificare anomalie che potrebbero indicare minacce sconosciute o attacchi complessi. L'analisi dei log gestita anche tramite servizio esterno SOC (security operation center) include:

- correlazione di eventi provenienti da fonti diverse (es. login fallito su VPN seguito da accesso anomalo su file server)
- rilevamento di deviazioni rispetto alla baseline di traffico o attività utente (User and Entity Behavior Analytics - UEBA)
- verifica della continuità e integrità dei flussi di log per rilevare tentativi di disabilitazione dei sistemi di monitoraggio

6 STRATEGIA PER LA GESTIONE DELLE VULNERABILITA' TECNICHE

La gestione delle vulnerabilità tecniche comprende attività di identificazione, analisi, classificazione, prioritizzazione e trattamento delle vulnerabilità che interessano sistemi, applicazioni, reti e dispositivi.
Viene adottato un processo di Coordinated Vulnerability Disclosure, assicurando che le segnalazioni di vulnerabilità ricevute da soggetti interni o esterni siano valutate, trattate e tracciate in modo strutturato.

6.1 IDENTIFICAZIONE DELLE VULNERABILITA'

E' necessario:

- Effettuare scansioni di vulnerabilità regolari sui sistemi del Comune di Parma per identificare potenziali punti deboli.
- Utilizzare servizi e fonti di threat intelligence per ottenere informazioni tempestive e contestualizzate sulle minacce e sulle vulnerabilità rilevanti, in coerenza con A.5.7 della ISO/IEC 27002:2022.
  - A.8.8 Gestione delle vulnerabilità tecniche: acquisizione tempestiva delle informazioni, valutazione dell'esposizione e adozione di misure appropriate;
  - A.8.9 Gestione della configurazione: definizione di baseline sicure, controllo delle modifiche e individuazione delle deviazioni che possono generare vulnerabilità;
  - A.8.16 Attività di monitoraggio: rilevazione e correlazione di eventi, anomalie e tentativi di sfruttamento delle vulnerabilità;

Il monitoraggio include l'iscrizione ai bollettini di sicurezza dei fornitori critici (es. Microsoft) per recepire tempestivamente le vulnerabilità "Zero-Day" o note che impattano la catena di approvvigionamento software.

I fornitori critici e le terze parti devono adottare processi strutturati di gestione delle vulnerabilità, notificare e risolvere tempestivamente le vulnerabilità che impattano i servizi contrattualizzati.

6.2 VALUTAZIONE DELLE VULNERABILITA'

- Classificare le vulnerabilità in base al rischio, considerando probabilità di sfruttamento e impatto potenziale su disponibilità, riservatezza e integrità dei dati.

- Utilizzare framework di classificazione standard come CVSS (Common Vulnerability Scoring System).

6.3 TRATTAMENTO DELLE VULNERABILITA'

E' necessario:

- Applicare patch o aggiornamenti e documentare le azioni correttive. I tempi di remediation sono determinati in base a criticità, esposizione, sfruttamento attivo, rilevanza dell'asset e impatto sul servizio; gli SLA riportati di seguito costituiscono obiettivi massimi, salvo termini più restrittivi derivanti dal rischio o da obblighi contrattuali e normativi.
  - Critica (CVSS 9.0-10): entro 72 ore dal rilascio della patch (o applicazione di workaround immediato).
  - Alta (CVSS 7.0-8.9): entro 7 giorni.
  - Media/Bassa: entro 30 giorni o alla successiva finestra di manutenzione programmata.

  Nel caso di sistemi critici per i servizi essenziali, qualora la patch non sia applicabile immediatamente, è obbligatorio implementare misure compensative documentate (es. segmentazione rete, Virtual Patching tramite WAF/IPS).
- Implementare misure di mitigazione come l'isolamento dei sistemi vulnerabili o il rafforzamento delle difese di rete in caso di vulnerabilità non risolvibili immediatamente.
- Monitorare periodicamente la conformità delle patch e le misure di sicurezza adottate.

6.4 MONITORAGGIO E REVISIONE

- Monitorare in continuo i sistemi per eventuali nuovi rischi, utilizzando strumenti di analisi comportamentale e di rilevamento delle anomalie.
- Effettuare audit periodici sulla gestione delle vulnerabilità e documentare le azioni di miglioramento richieste.

6.5 THREAT INTELLIGENCE

- Creare un processo di Threat Intelligence che comprenda la raccolta e l'analisi delle informazioni sulle minacce da fonti pubbliche e commerciali.
- Integrare la threat intelligence nelle valutazioni di rischio e condividere con il Team IT le informazioni rilevanti per la protezione dei sistemi del Comune di Parma.

6.6 DIVULGAZIONE COORDINATA DELLE VULNERABILITA' (CVD) (ART. 16 D.LGS. 138/2024)

Viene adottata una politica di divulgazione coordinata. Le segnalazioni di vulnerabilità provenienti da ricercatori esterni o terze parti sono gestite secondo principi di responsabilità e non divulgazione pubblica fino alla risoluzione.

l'Ente si impegna a:

- mantenere la riservatezza sull'identità del segnalante;
- non intraprendere azioni legali contro ricercatori etici che operano nel rispetto delle policy aziendali e senza causare danni a servizi.

7 FORMAZIONE E SENSIBILIZZAZIONE DEGLI UTENTI

E' necessario:

- Erogare formazione periodica a tutti gli utenti sul riconoscimento delle minacce comuni, incluse phishing e social engineering.
- Sensibilizzare i dipendenti sulla politica di gestione delle vulnerabilità, specificando le azioni preventive da adottare in caso di situazioni sospette.
- Fornire aggiornamenti regolari ai dipendenti su nuove minacce e vulnerabilità tramite newsletter interne e workshop.

8 MONITORAGGIO, KPI E MIGLIORAMENTO CONTINUO

Vengono definiti e monitorati indicatori di prestazione (KPI) relativi alla gestione delle vulnerabilità, tra cui il numero di vulnerabilità critiche, i tempi di remediation, la copertura delle scansioni e l'andamento del rischio residuo. I risultati sono riesaminati periodicamente.

9 DOCUMENTAZIONE E REPORTING

Ogni attività di gestione delle vulnerabilità deve essere documentata e archiviata per fini di audit. Gli incidenti e gli eventi derivanti dallo sfruttamento di vulnerabilità sono registrati, analizzati e comunicati al RTD e agli Organi di Amministrazione e Direttivi secondo la Procedura di Gestione degli Incidenti, affinché siano valutate le azioni di miglioramento e gli eventuali obblighi di notifica. Il reporting evidenzia le vulnerabilità critiche non risolte entro gli SLA, le eccezioni, le misure compensative e il rischio residuo. Le decisioni di accettazione del rischio sono formalizzate dagli organi competenti del Comune, sono limitate nel tempo e sono collegate al al Piano di Trattamento/ Adeguamento.

10 REVISIONE DELLA POLITICA

Questo Piano sarà riesaminato annualmente o ogni qualvolta siano introdotte modifiche significative nei sistemi o nei processi aziendali o in caso di incidente significativo, per garantire la sua continua efficacia e conformità con lo standard ISO/IEC 27001:2022 e alla Direttiva NIS2.

11 CONTATTI E SUPPORTO

Per ulteriori informazioni sulla gestione delle vulnerabilità o per segnalare una vulnerabilità, contattare il Responsabile della Sicurezza IT all'indirizzo servizi.informatici@comune.parma.it sistemi@itcity.it o il Settore compente in materia ICT.

12 PRESIDI INTEGRATIVI ISO/IEC 27001:2022 E NIS2

12.1 COLLEGAMENTO CON IL RISCHIO E LA DICHIARAZIONE DI APPLICABILITÀ

Ogni vulnerabilità rilevante è collegata all'asset, al servizio o processo interessato, al relativo proprietario, allo scenario della Valutazione del Rischio e ai controlli applicabili. Le vulnerabilità che determinano un rischio non accettabile generano un'azione di trattamento nel Piano di Adeguamento o un intervento urgente, con responsabile, scadenza, evidenza di chiusura e verifica del rischio residuo.

12.2 PERIMETRO, INVENTARIO E FONTI DI RILEVAZIONE

Il perimetro di scansione e verifica deriva dall'inventario degli asset e include, secondo applicabilità, sistemi interni ed esposti, cloud, applicazioni web, API, dispositivi di rete e sicurezza, endpoint, database, componenti software, librerie, immagini e container, codice sviluppato internamente o da fornitori e configurazioni. Per ciascun asset sono registrati proprietario, criticità, esposizione, ambiente, fornitore, stato di supporto e finestra autorizzata di verifica.

Le fonti comprendono scansioni autenticata e non autenticata, penetration test autorizzati, strumenti EDR/XDR e CSPM, code e dependency scanning, bollettini ACN/CSIRT Italia, advisory dei produttori e dei fornitori, CVE e ulteriori fonti qualificate, attività SOC, incidenti e segnalazioni CVD (divulgazione coordinata delle vulnerabilità). Le verifiche sono pianificate per evitare impatti sui servizi e sono eseguite esclusivamente con autorizzazione e regole di ingaggio documentate.

12.3 VALUTAZIONE E PRIORITIZZAZIONE BASATA SUL RISCHIO

Il punteggio CVSS (sistema per la valutazione delle gravità delle vulnerabilità) è un input e non costituisce l'unico criterio. La priorità considera sfruttamento attivo o disponibilità di exploit, esposizione a Internet, privilegi richiesti, criticità del servizio, classificazione delle informazioni, numero e tipologia di utenti interessati, dipendenze, possibilità di movimento laterale, efficacia dei controlli compensativi, stato di supporto e impatti operativi, economici, normativi e verso terzi.

Le vulnerabilità su servizi essenziali o importanti, sistemi di autenticazione, infrastrutture di sicurezza, asset esposti e componenti condivisi sono sottoposte a valutazione accelerata. Le vulnerabilità con rischio elevato o sfruttamento attivo sono immediatamente comunicate al RTD e al presidio incidenti, anche prima del completamento dell'analisi ordinaria.

12.4 REMEDIATION, CONFIGURAZIONE E SVILUPPO SICURO

Le principali fasi del processo di remediation sono:

- applicare patch e correzioni mediante change management, prevedendo test proporzionati, backup o punto di ripristino, piano di rollback e verifica post-intervento;
- gestire le emergenze con procedure accelerate e separazione delle responsabilità compatibile con la criticità;
- adottare baseline di configurazione sicura e verificare periodicamente le deviazioni, in coerenza con A.8.9;
- validare la chiusura mediante nuova scansione, verifica manuale o evidenza equivalente e aggiornare il rischio residuo;

- per sviluppi interni o affidati a fornitori, applicare requisiti di codifica sicura, analisi del codice e delle dipendenze, gestione dei segreti e correzione delle vulnerabilità prima del rilascio, in coerenza con A.8.28;
- ove applicabile, mantenere l'inventario delle componenti software o evidenze equivalenti per agevolare l'analisi dell'impatto delle vulnerabilità di filiera.

Qualora una patch non sia disponibile o non possa essere applicata nei tempi previsti, sono attuate misure compensative documentate, quali segmentazione, limitazione degli accessi, disabilitazione della funzione, virtual patching, incremento del monitoraggio o isolamento. L'eccezione indica motivazione, rischio, responsabile, termine, piano di rientro e approvazione competente.

12.5 CLOUD, FORNITORI E NOTIFICA A CASCATA

Per servizi cloud e gestiti sono definite le responsabilità del Comune, di IT.CITY S.p.A. e del fornitore, le modalità di accesso alle evidenze, i requisiti di hardening e logging, i tempi di comunicazione e remediation, la gestione delle vulnerabilità delle componenti sottostanti e le modalità di verifica. I rischi specifici sono trattati in coerenza con A.5.23 e con il processo di valutazione dei fornitori.

I contratti con fornitori e subfornitori prevedono la comunicazione tempestiva a cascata di vulnerabilità, compromissioni e incidenti che possano interessare i servizi del Comune, con informazioni e tempi idonei a consentire la valutazione e, se necessario, la pre-notifica al CSIRT Italia entro 24 ore. Sono previsti obblighi di cooperazione, aggiornamento, conservazione delle evidenze e supporto alla root cause analysis.

12.6 MONITORAGGIO, INCIDENTI E THREAT INTELLIGENCE

Le informazioni di threat intelligence di cui ad A.5.7 alimentano la selezione degli asset da verificare, la frequenza delle scansioni, la prioritizzazione e le regole di monitoraggio. Le attività di logging, SOC e correlazione di cui ad A.8.16 sono aggiornate per rilevare tentativi di sfruttamento e per verificare l'efficacia delle misure compensative.

Lo sfruttamento riuscito o sospetto di una vulnerabilità è gestito come evento o incidente secondo la Procedura di Gestione degli Incidenti. La classificazione di incidente significativo considera grave perturbazione operativa o perdite finanziarie e ripercussioni materiali o immateriali considerevoli su persone fisiche o giuridiche; la procedura disciplina pre-notifica entro 24 ore, notifica entro 72 ore e relazione finale entro un mese.

12.7 KPI, REPORTING, RIESAME E MIGLIORAMENTO

Sono monitorati almeno: copertura e frequenza delle scansioni, percentuale di asset inventariati e verificati, numero di vulnerabilità per criticità, tempo medio e massimo di presa in carico e remediation, percentuale di rispetto degli SLA, vulnerabilità riaperte, eccezioni e loro anzianità, efficacia delle misure compensative, esposizioni dei fornitori e trend del rischio residuo.

Il RTD riceve reporting periodico e tempestivo per le esposizioni critiche; gli Organi di Amministrazione e Direttivi ricevono informazioni sufficienti a esercitare approvazione e supervisione, allocare risorse e autorizzare le eccezioni. Gli esiti alimentano riesame, audit, Valutazione del Rischio, Piano di Trattamento/Adeguamento e formazione. Il documento è riesaminato almeno annualmente e in caso di incidente significativo, vulnerabilità critica, variazione di fornitori o cloud, introduzione di nuove tecnologie, modifica normativa o risultato insoddisfacente degli indicatori.

Il presente ciclo assicura coerenza con le clausole 4-10 della ISO/IEC 27001:2022: contesto e perimetro, leadership e responsabilità, pianificazione basata sul rischio, risorse e competenze, operatività controllata, valutazione delle prestazioni e miglioramento continuo.