❑ DOCUMENTO PUBBLICO	■ AD USO INTERNO	❑ RISERVATO

COMUNE DI NAPOLI

Modello di Governance del Comune di Napoli

(Legge n. 90/2024 e D.Lgs. n. 138/2024)

❑ DOCUMENTO PUBBLICO	■ AD USO INTERNO	❑ RISERVATO

COMUNE DI NAPOLI

Emissione del Documento

	Nome	Ruolo
Redazione	Francesco Essolito	EQ “Staff al Responsabile della Transizione Digitale e Cybersecurity a livello di Ente”
Verifica organizzativa	Lucio Abbate	Dirigente Servizio Gestione Sistemi e Reti Tecnologiche
Approvazione	Vincenzo Ferrara	Responsabile Area Digitalizzazione e Sistemi Informativi

Elenco delle modifiche del documento

Versione	Data	Autore	Dettagli
1.0	20/10/2025	Area Digitalizzazione e Sistemi Informativi	Prima versione del documento

INDICE

1. INTRODUZIONE

1.1 Obiettivo del Documento

Il presente documento ha l'obiettivo di illustrare le linee strategiche, gli obiettivi prefissati e le conseguenti attività da porre in essere in merito alla sicurezza di dati, sistemi e alle infrastrutture del Comune di Napoli, al fine di assicurare la conformità alle leggi e alle normative vigenti, con particolare riferimento all'articolo 8 della legge n. 90/2024, entrata in vigore il 17 luglio 2024 (di seguito Legge), inerente al rafforzamento della resilienza delle pubbliche amministrazioni ed all'individuazione del Referente per la cybersicurezza. Il documento, inoltre, è ritenuto propedeutico anche ai fini del recepimento di quanto richiesto dal D.Lgs. n. 138 del 4/9/2024, relativo al recepimento della direttiva (UE) 2022/2555 cd. "NIS2".

1.2 Ambito di Applicazione

Il presente documento si applica al Comune di Napoli in quanto rientrante nei soggetti individuati dalla Legge ex art. 1 comma 3. Nello specifico, il Modello Organizzativo deve essere promosso attivamente dall'Amministrazione competente e rispettato da tutti i dipendenti del Comune di Napoli con riferimento a tutte le attività legate alla gestione della sicurezza delle informazioni e dei sistemi informatici.

2. RIFERIMENTI NORMATIVI

I riferimenti normativi e documentali alla base del presente Modello sono:

- Legge 28 giugno 2024, n. 90;
- D. Lgs. 30 marzo 2001, n. 165;
- D. Lgs. 7 marzo 2005, n. 82;
- D.l 21 settembre 2019, n. 105;
- D. Lgs. del 4 settembre 2024, n. 138;
- ACN-GPDP, Linee guida funzioni crittografiche;
- Determinazione ACN 164179 del 14 aprile 2025 – "*Specifiche di base per l'adempimento agli obblighi di cui agli articoli 23, 24, 25, 29 e 32 del decreto NIS per i soggetti importanti*".

3. DEFINIZIONI, ABBREVIAZIONI E ACRONIMI

Termine/Abbreviazione	Definizione
ACN	Agenzia per la cybersicurezza nazionale
ARDI	Area Digitalizzazione e Sistemi Informativi
AgID	Agenzia per l'Italia Digitale
CSIRT	Computer Security Incident Response Team
GDPR	General Data Protection Regulation (Regolamento 2016/679)

IRP	Incident Response Plan
Need To Know	Principio di sicurezza secondo il quale ciascun utente deve essere a conoscenza delle sole informazioni a lui necessarie per lo svolgimento delle sue attività lavorative
Least Privilege	Principio di sicurezza secondo il quale ad un utente viene concesso il privilegio minimo indispensabile che consente il livello di accesso necessario a svolgere le attività lavorative di sua competenza
PPSI	Piano Programmatico di Sicurezza Informatica
PT	Penetration Test
Q&A	Situazione in cui durante un evento una persona o un gruppo di persone pone domande e un'altra persona o un gruppo di persone risponde rispetto ad un tema trattato
Segregation of Duties	Principio secondo il quale i compiti e le aree di responsabilità in conflitto tra loro devono essere separati per ridurre le possibilità di uso improprio, modifica non autorizzata o non intenzionale degli asset di un'organizzazione
Supply Chain	In italiano "catena di approvvigionamento", si riferisce al sistema di tutte le attività, organizzazioni, persone, informazioni e risorse coinvolte nell'intero processo, dalle materie prime alla consegna del prodotto finale ai consumatori
SW	Software
VA	Vulnerability Assessment
SOC	Security Operation Center

4. RUOLI E RESPONSABILITÀ

La sezione descrive, in modo chiaro e sintetico, ruoli e responsabilità degli attori cardine dell'organizzazione per la sicurezza informatica definita dal Comune di Napoli, descritta nel dettaglio nei seguenti paragrafi.

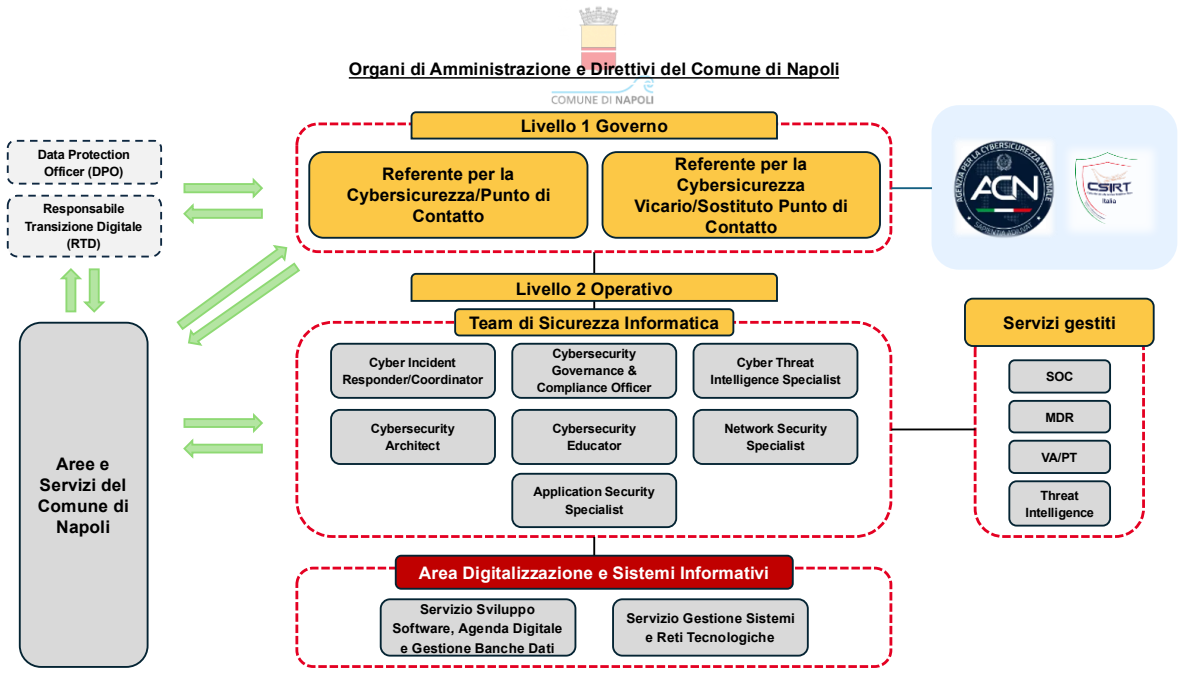
Organi di Amministrazione e Direttivi	Gli Organi di Amministrazione e Direttivi promuovono la cultura della sicurezza delle informazioni e approvano le modalità d'implementazione delle misure di sicurezza, sovrintendono all'implementazione degli obblighi e sono responsabili di eventuali violazioni e non osservanza della normativa vigente in materia di cybersicurezza.
Dirigenti	I Dirigenti si impegnano a far rispettare il presente documento e i documenti che ne discenderanno, a tutti i dipendenti a loro sottoposti ed a svolgere un ruolo di indirizzo e controllo delle strategie di sicurezza informatica promosse dal Comune di Napoli.
Dipendenti	I dipendenti di ogni livello del Comune di Napoli si

	impegnano a contribuire alla sicurezza informatica dell'Ente rispettando le direttive della presente policy e delle successive policies che ne discenderanno, ed attuando le procedure di sicurezza applicabili.
Soggetti esterni	Tutti i fornitori esterni, Consulenti, Partner o qualsiasi soggetto autorizzato ed abilitato ad accedere a risorse informative o ad utilizzare servizi informatici del Comune di Napoli si impegnano a far rispettare il presente documento.
Referente per la Cybersicurezza (in adempimento alla Legge 90/2024) **Punto di Contatto (in adempimento al D. Lgs. n. 138/2024)**	Persona incaricata di sviluppare e implementare le politiche e le procedure di sicurezza informatica, nonché punto di contatto primario dell'Amministrazione con l'Agenzia per la Cybersicurezza Nazionale (ACN), in relazione a quanto previsto dalle normative vigenti in materia di cybersicurezza, cui è soggetto il Comune di Napoli.
Referente per la Cybersicurezza vicario (in adempimento alla Legge 90/2024) **Sostituto Punto di Contatto (in adempimento al D. Lgs. n. 138/2024)**	Persona incaricata di affiancare ed eventualmente sostituire, in caso di assenza o impedimento, il Referente per la Cybersicurezza nello svolgimento degli incarichi ad esso assegnati nell'ambito di quanto previsto dalle normative vigenti in materia di cybersicurezza, cui è soggetto il Comune di Napoli.
Team di Sicurezza Informatica	Gruppo di esperti che supporta il Referente per la Cybersicurezza nelle attività finalizzate a proteggere i sistemi informatici, le reti e i dati dell'Ente da minacce e attacchi informatici attraverso, ad esempio, attività di monitoraggio, la risposta agli incidenti ecc.
Area Digitalizzazione e Sistemi Informativi	L'ARDI del Comune di Napoli gestisce e coordina tutte le attività legate ai sistemi informativi e alle tecnologie dell'informazione. I suoi compiti principali includono la pianificazione strategica IT, la gestione delle infrastrutture tecnologiche, la sicurezza informatica, il supporto tecnico ai dipendenti, la gestione dei progetti IT, il supporto alle attività di formazione del personale nonché l'innovazione tecnologica e la conformità alle normative vigenti in materia di sicurezza informatica.

5. MODELLO ORGANIZZATIVO

Al fine di rafforzare la resilienza dell'Amministrazione in conformità con quanto previsto dalla Legge 90/2024 all'art. 8 e dal D.lgs. 138/2024 all'art. 24, il Comune di Napoli ha definito un apposito **Modello Organizzativo** allo scopo di pianificare, coordinare e porre in essere le attività in materia di cybersicurezza.

Come previsto dalla normativa, il Comune di Napoli ha identificato gli organi di Amministrazione e Direttivi responsabili delle decisioni strategiche dell'Ente e delegati alla supervisione della concreta attuazione delle misure di gestione e prevenzione dei rischi adottate. All'interno del predetto Modello è stato inoltre designato un **Referente per la Cybersicurezza/Punto di Contatto**, individuato tra il personale in ragione di specifiche e comprovate professionalità, il cui nominativo è comunicato all'Agenzia per la Cybersicurezza Nazionale, nonché un **Referente per la Cybersicurezza Vicario/Sostituto Punto di Contatto**, con il ruolo di normale affiancamento ed eventuale sostituzione in caso di assenza o impedimento del Referente principale. Il Referente per la Cybersicurezza/Punto di Contatto, con il supporto del Referente per la Cybersicurezza Vicario/Sostituto Punto di Contatto e unitamente al **Team di Sicurezza** individuato – composto da risorse dotate delle competenze di seguito riportate e dall'Area Digitalizzazione e Sistemi Informativi del Comune di Napoli che lo supporta – è responsabile delle attività che sono meglio descritte nei successivi paragrafi. Tale modello include inoltre la responsabilità delle diverse Aree e Servizi del Comune di Napoli coinvolte nella gestione dei processi, coadiuvate dal Data Protection Officer e dal Responsabile per la Transizione Digitale rispettivamente nella gestione degli aspetti legati alla protezione dei dati personali e alla digitalizzazione dei processi amministrativi, in quanto si presuppone l'esistenza di una responsabilità condivisa al fine del conseguimento di un adeguato livello di sicurezza informatica.



5.1 Organizzazione del sistema di sicurezza delle informazioni

Il Comune di Napoli, in conformità con quanto previsto dalla Legge all'art. 8 comma 1 c) e dall'art. 24 del D.lgs 138/2024, al fine di garantire che tutte le attività di sicurezza informatica siano coordinate, efficaci e allineate con gli obiettivi posti dall'Ente, definisce ed organizza le attività di sicurezza delle informazioni poste in essere dall'Organizzazione del sistema di sicurezza delle informazioni del Comune di Napoli.

L'organizzazione del sistema di sicurezza delle informazioni si struttura su due livelli:

a) **Livello di Governo**: rappresenta il primo livello organizzativo e tecnico del sistema di sicurezza delle informazioni ed è sorretto dal Referente per la Cybersicurezza/Punto di Contatto. Il Referente, nominato mediante apposita delibera emessa dall'Amministrazione e individuato tra il personale dipendente in ragione di specifiche e comprovate professionalità nonché competenze in materia di cybersicurezza, rappresenta la principale figura di riferimento del Comune per la gestione di tutte le tematiche inerenti alla cybersicurezza dell'Ente. Pertanto, al fine di garantire un adeguato livello di sicurezza informatica, tutte le Aree e Servizi del Comune di Napoli collaborano con il Referente per la Cybersicurezza/Punto di Contatto, il quale supervisiona, gestisce e coordina le attività di sicurezza informatica.
b) **Livello Operativo**: rappresenta il secondo livello del sistema di sicurezza delle informazioni ed è composto dalle funzioni che si occupano della gestione operativa della sicurezza. Questo livello con il coordinamento dal livello di governo assicura l'implementazione e l'esecuzione delle attività di sicurezza dell'Ente, ed è costituito da personale dipendente dotato di specifiche e comprovate professionalità e competenze in materia di cybersicurezza, organizzato nell'apposito **Team di Sicurezza Informatica**.

In tale contesto il **Team di Sicurezza Informatica** del Comune di Napoli svolge un ruolo cruciale, un presidio costante e continuativo nella protezione delle risorse informatiche e dei dati digitali gestiti dal Comune di Napoli. Le responsabilità di questo team variano a seconda degli ambiti di intervento a cui fa riferimento una specifica figura professionale, avente una competenza ed una responsabilità di coordinamento ben definita. Di seguito, il dettaglio relativo al Team di Sicurezza Informatica, con una descrizione dei principali compiti assunti da ciascuna competenza identificata.

<u>Team di Sicurezza Informatica</u>

- **Cyber Incident Responder/Coordinator**: È responsabile della gestione e coordinamento delle attività relative agli incidenti di sicurezza informatica all'interno dell'Ente e collabora con il SOC. Questo professionista svolge un ruolo cruciale nel garantire una risposta tempestiva ed efficace agli attacchi informatici, minimizzando gli impatti e ripristinando la normale operatività dei sistemi ICT.
- **Cybersecurity Governance & Compliance Officer**: Sovraintende e garantisce la conformità della cybersicurezza con le normative interne dell'organizzazione (regolamenti, politiche e procedure), con le normative esterne (leggi e regolamenti), e con framework/standard internazionali. Inoltre, contribuisce ad individuare le azioni necessarie per garantire la protezione dei dati e le strategie di rimedio per garantire la conformità. Ha

un ruolo di supporto nello sviluppo dei processi di governance della cybersicurezza dell'organizzazione.

- **Cyber Threat Intelligence Specialist**: Coordina il ciclo di vita della Cyber Threat Intelligence, che comprende la raccolta di informazioni relative alle minacce informatiche, l'analisi e la produzione di informazioni di intelligence utilizzabili nonché la diffusione delle stesse verso gli stakeholder interni che si occupano di cybersicurezza e verso la comunità CTI, a livello tattico, operativo e strategico. Inoltre, provvede a identificare e monitorare le tattiche, le tecniche e le procedure utilizzate dagli attori delle minacce informatiche ed i relativi "trend", tracciare le attività degli attaccanti e osservare come gli eventi non informatici possono influenzare la postura di cybersicurezza.
- **Cybersecurity Architect**: Coordina la progettazione di soluzioni basate su principi di sicurezza e privacy (per esempio Privacy by Design e by Default e Security by Design e by Default) in relazione a infrastrutture, sistemi, asset, licenze software, hardware e servizi, e di progettare controlli di cybersicurezza che ne confermino l'applicazione.
- **Cybersecurity Educator**: È responsabile della progettazione, implementazione e gestione dei programmi di formazione in materia di sicurezza informatica all'interno dell'Ente. Questo professionista ha il compito di sensibilizzare e coordinare le attività formative su tematiche di cybersecurity, promuovendo una cultura della sicurezza e riducendo i rischi associati a comportamenti imprudenti. Questa figura agisce in collaborazione con la struttura preposta alla programmazione delle attività formative nell'ambito delle Risorse Umane.
- **Network Security Specialist**: Coordina la protezione delle reti informatiche dell'organizzazione, garantendo la sicurezza dei dati e delle comunicazioni. Questo professionista si occupa di progettare, implementare e gestire soluzioni di sicurezza per prevenire accessi non autorizzati, attacchi informatici e altre minacce alla rete.
- **Application Security Specialist:** Coordina la progettazione di soluzioni applicative basate su principi di sicurezza e privacy (per esempio Privacy by Design e by Default e Security by Design e by Default) e le attività di valutazione della sicurezza delle applicazioni sia di quelle acquistate (esterne) sia di quelle realizzate in proprio (interne), garantendo che il software sia sviluppato e conforme con le migliori pratiche di sicurezza, definisce e revisiona i test per quelle esterne e interne.

Per tutte le attività inerenti al processo di gestione degli incidenti informatici, il Team di Sicurezza Informatica è affiancato dal **SOC del Comune di Napoli**. Attraverso un monitoraggio costante degli eventi di sicurezza informatica, il SOC ha il compito di identificare tempestivamente attività anomale o potenziali minacce. In caso di incidenti, interviene con analisi approfondite e misure di contenimento, limitando i danni e riducendo al minimo l'impatto sulle operazioni quotidiane, nonché garantendo un recupero in tempi brevi dei sistemi impattati e delle loro funzionalità.

Il Team di Sicurezza Informatica preposto, si avvale delle competenze operative e strategiche dell'Area Digitalizzazione e Sistemi Informativi che con delibera n. 080 del 23/12/2024, ha individuato due Servizi volti a garantire l'efficacia, l'efficienza, l'allineamento con gli obiettivi strategici dell'Ente nonché la conformità alle normative, standard di sicurezza e best practices di cybersecurity dei processi di sicurezza loro attribuiti:

a. *Servizio Sviluppo Software, Agenda Digitale e Gestione Banche Dati – ARDI1041;*
b. *Servizio Gestione Sistemi e Reti Tecnologiche – ARDI1042.*

I due Servizi sono parte attiva dei processi di sicurezza identificati dal Comune, di seguito esplicitati:

Processi di Sicurezza

a) ***Security Operations***: Attività finalizzate a garantire la protezione e il funzionamento sicuro delle infrastrutture IT attraverso il monitoraggio delle reti e dei server, la gestione delle vulnerabilità con l'applicazione di patch e la configurazione di dispositivi di sicurezza. L'operatività include la gestione delle postazioni di lavoro in conformità alle normative, il censimento e la classificazione degli asset, e la protezione dei dati aziendali. Viene inoltre curata l'amministrazione dei profili applicativi, con l'integrazione di metodi avanzati di autenticazione per rafforzare la sicurezza degli accessi. La supervisione dell'Active Directory comprende la gestione delle utenze, delle credenziali e dei privilegi, oltre al monitoraggio dei log per l'individuazione di attività sospette. Infine, le attività si estendono alla gestione dell'infrastruttura server, al controllo degli impianti tecnologici e alla protezione fisica delle risorse, assicurando la continuità operativa attraverso strategie di Disaster Recovery.
b) ***Security Incident Management***: Attività finalizzate a garantire il rilevamento degli incidenti attraverso il monitoraggio continuo delle reti e dei sistemi, individuando attività sospette e potenziali minacce alla sicurezza. L'analisi e il contenimento degli eventi critici permettono di mitigare i rischi per l'organizzazione, assicurando una risposta tempestiva ed efficace. Viene coordinato il ripristino dei sistemi e della normale operatività a seguito di un incidente, garantendo la continuità delle attività aziendali. Infine, la conduzione di post-incident review consente di analizzare le cause degli eventi, trarre insegnamenti utili e implementare misure preventive per evitare episodi futuri.
c) ***Business Continuity Management***: Attività finalizzate a garantire la gestione e l'amministrazione della Server Farm, comprendendo l'identificazione dei processi e servizi critici dell'Ente, l'implementazione di piani di continuità operativa e la conduzione di Business Impact Analysis con definizione di RTO e RPO. Viene inoltre assicurata l'attuazione delle politiche di backup per la protezione dei dati e la definizione di piani di Disaster Recovery per ripristinare i sistemi in caso di eventi critici.
d) ***Cyber Security Governance e Compliance***: Attività finalizzate a garantire la definizione di strategie di sicurezza delle informazioni in linea con gli indirizzi dell'Ente, l'adeguamento alle normative nazionali ed europee, nonché la redazione e l'aggiornamento di policy e procedure di sicurezza. La gestione comprende la verifica della conformità agli standard di cybersecurity, il controllo degli audit per garantire l'adesione ai requisiti regolatori e il monitoraggio costante delle iniziative di sicurezza. Inoltre, vengono identificate le attività critiche dell'Ente, analizzati i rischi secondo la metodologia definita e sviluppati piani di trattamento o accettazione del rischio. Il monitoraggio continuo assicura l'effettiva implementazione delle misure correttive per la protezione e la resilienza dell'organizzazione.

e) ***Supply Chain Management***: Attività finalizzate a garantire la gestione sicura delle Terze Parti attraverso la definizione di linee guida e requisiti di cybersecurity necessari per proteggere la fornitura, con verifiche sulla conformità alle policy aziendali e controlli periodici per monitorare i rischi nella catena di approvvigionamento. Inoltre, viene supportata la quantificazione e allocazione delle risorse economiche per la sicurezza informatica mediante l'analisi delle esigenze di information security, la valutazione dei costi e la pianificazione degli investimenti, assicurando un uso efficiente del budget e l'efficacia delle iniziative di protezione.

g) ***Cybersecurity Intelligence****:* Attività finalizzate alla raccolta e analisi dei dati sulle minacce emergenti e sulle nuove tecniche di attacco informatico, attraverso il monitoraggio di fonti interne ed esterne per identificare trend e indicatori di compromissione, adattando proattivamente le strategie di difesa. L'analisi delle informazioni di intelligence consente la produzione di report dettagliati e l'elaborazione di piani di mitigazione tattici per rafforzare la sicurezza dell'organizzazione.

h) ***Security by Default & by Design****:* Attività finalizzate a garantire la sicurezza nelle fasi di progettazione e sviluppo di soluzioni tecnologiche, attraverso la definizione dei requisiti di cybersecurity e l'implementazione di pratiche di sviluppo sicuro. L'analisi e la progettazione di architetture dati consentono la realizzazione e gestione di un datawarehouse, favorendo l'integrazione e l'analisi tra le banche dati dell'Ente per supportare la pianificazione e i processi decisionali. Inoltre, vengono condotte analisi sul potenziale delle tecnologie emergenti applicabili all'Amministrazione comunale, tramite valutazioni di mercato, sperimentazione di strumenti innovativi e individuazione di ambiti di sviluppo. Infine, la gestione della sicurezza delle informazioni è garantita dall'implementazione di protocolli di cifratura per la protezione dei dati in transito e a riposo, oltre alla gestione delle chiavi crittografiche per preservare la confidenzialità e l'integrità delle informazioni.

i) ***Cybersecurity Training & Awareness***: Attività finalizzate a garantire la definizione di un piano di formazione periodico dell'Ente, conforme alle normative vigenti in materia di cybersecurity e data protection. L'iniziativa prevede programmi di formazione dedicati alle figure specialistiche, oltre a test e simulazioni mirati ad accrescere la consapevolezza del personale nell'identificazione e riconoscimento di potenziali incidenti di sicurezza.

5.2 Definizione di un piano programmatico per la sicurezza di dati, sistemi e infrastrutture

Il Comune di Napoli, in conformità con quanto previsto dalla Legge all'art. 8 comma 1 lettera d), sta lavorando alla definizione di un Piano Programmatico per la Sicurezza i Dati, Sistemi e Infrastrutture detto anche Piano Programmatico di Sicurezza Informatica (PPSI), al fine di adottare un approccio strutturato e sistematico alla protezione delle risorse informatiche e alle informazioni gestite dall'Ente, con l'obiettivo di prevenire, rilevare e rispondere efficacemente alle minacce di sicurezza informatica insistenti sul Comune.

Il Piano Programmatico di Sicurezza Informatica è un documento strategico fondamentale che guida il Comune di Napoli nella definizione di strategie di sicurezza delle informazioni. Il PPSI stabilisce le politiche di sicurezza informatica del Comune di Napoli, delineando le misure di sicurezza che l'Ente è chiamato ad implementare al fine di garantire la sicurezza informatica

nonché la conformità con standard, best practices e normative di settore, in funzione delle risorse disponibili per la sua attuazione.

Tra le varie misure di sicurezza individuate dal Piano, rilevano le attività finalizzate all'identificazione e valutazione dei rischi informatici. Nello specifico, il Piano guida il Comune di Napoli nella pianificazione e implementazione delle misure di sicurezza che devono essere adottate per mitigare i rischi identificati. Queste misure possono includere controlli di carattere tecnico, organizzativo e procedurale. Il Piano, inoltre, promuove iniziative per il monitoraggio continuo delle misure di sicurezza e per la revisione periodica delle stesse, affinché si assicuri l'efficace ed il corretto aggiornamento rispetto a nuove minacce informatiche, anche tenuto conto dei rischi e delle potenziali minacce derivanti dall'espletamento delle attività da parte dei fornitori di beni e servizi del Comune di Napoli.

In riferimento alla gestione degli eventi di sicurezza informatica, il PPSI definisce le iniziative a cui è chiamato il Comune di Napoli per la gestione degli incidenti di sicurezza, inclusa la definizione di puntuali piani di risposta e recupero, per minimizzare l'impatto di eventuali eventi pregiudizievoli.

Tra le iniziative previste dal PPSI rilevano le iniziative e i programmi di formazione continua per il personale. In particolare, il PPSI include programmi di formazione e sensibilizzazione per i dipendenti, al fine di garantire che questi comprendano l'importanza della sicurezza informatica e sappiano come comportarsi per garantire una gestione sicura e virtuosa delle risorse nonché delle attività a cui sono chiamati.

Il Piano Programmatico di Sicurezza Informatica prevede, infine, iniziative finalizzate a garantire il monitoraggio continuo ed il recepimento dei requisiti di sicurezza stabiliti dalle normative e dagli standard di sicurezza informatica applicabili all'Amministrazione, previsti dal legislatore nazionale e comunitario come, ad esempio, la Legge del 28 giugno 2024, n. 90, il Regolamento Europeo 2016/679 (GDPR) o il D.lgs. 138/2024 inerente al recepimento della Direttiva Europea 2022/2555, circa le misure per un livello comune elevato di cybersicurezza nell'Unione.

5.3 Sviluppo politiche e procedure di sicurezza delle informazioni

Il Comune di Napoli, in conformità con quanto previsto dalla Legge all'art. 8, comma 1 lettera a), mediante la propria struttura organizzativa sopra descritta, nella veste del Referente per la Cybersicurezza/Punto di Contatto nonché del Team a suo supporto, promuove lo sviluppo di politiche e procedure di sicurezza delle informazioni.

5.4 Adozione linee guida per la cybersicurezza

Il Comune di Napoli, in conformità con quanto previsto dalla Legge all'art. 8 comma 1 lettera f) in sede di attuazione e adozione delle misure previste dalle linee guida per la cybersicurezza, redige e aggiorna il proprio corpo documentale, al fine di recepire gli orientamenti dell'ACN nonché attuare misure di sicurezza informatica tese al rafforzamento della security posture dell'Ente.

Il Comune di Napoli, inoltre, in conformità con l'art. 24 del D.lgs 138/2024, ha implementato una serie di misure di sicurezza tecniche avanzate come l'adozione di firewall robusti, sistemi per rilevare le intrusioni e software antivirus per il monitoraggio continuo delle reti e dispositivi, e per rilevare e neutralizzare tempestivamente eventuali minacce. Inoltre, sono presenti sistemi di controllo accessi per garantire che solo il personale autorizzato possa accedere alle informazioni riservate. Le iniziative sopra descritte rappresentano l'impegno profuso dall'Ente per mantenere l'ecosistema digitale comunale sicuro, in linea con le migliori pratiche del settore e con le normative vigenti. A tal proposito, l'Ente ha definito e adottato misure di sicurezza puntuali per il rilevamento di eventi impattanti la sicurezza informatica dell'Ente. In particolare, nel caso di eventi di sicurezza è stato definito un processo per la segnalazione degli stessi, in conformità con la relativa procedura di gestione degli incidenti di sicurezza. La procedura definisce le modalità adottate dall'Area Digitalizzazione e Sistemi Informativi dell'Ente per assicurare la corretta gestione degli incidenti, ovvero gli interventi e le attività tecniche da porre in risposta agli eventi impattanti la sicurezza dell'Ente. Nello specifico, l'Area Digitalizzazione e Sistemi Informativi ha definito un IRP al fine di descrivere i comportamenti che il personale dipendente deve seguire per una risposta immediata ed efficace.

5.5 Gestione del rischio informatico

Il Comune di Napoli, in conformità con quanto previsto dalla Legge all'art. 8, comma 1 lettera b) e dall'art. 24 del D.lgs 138/2024, ha avviato la definizione di un processo di analisi e gestione dei rischi di cybersecurity che prevede diverse fasi cruciali per la protezione delle risorse e delle informazioni gestite dal Comune di Napoli. L'implementazione e l'esecuzione del processo è soggetta alla possibilità di avvalersi di un supporto esterno (Fornitori di servizi ICT) al fine di garantire l'espletamento delle attività riportate di seguito.

L'approccio promosso dall'Ente, relativamente alla gestione dei rischi di cybersecurity, si pone quale obiettivo quello di garantire la continuità operativa dei servizi essenziali e non, in un contesto di minacce informatiche sempre più sofisticate e in continua evoluzione. Pertanto, al fine di agevolare e guidare il personale dell'Ente nella gestione del rischio informatico, l'Area Digitalizzazione e Sistemi Informativi ha definito una Metodologia di Cyber Risk Management. Il processo prevede una prima fase di analisi del contesto, finalizzato alla valutazione del rischio sui processi identificati, esaminando i fattori interni ed esterni ai processi stessi. Questo passo è fondamentale per comprendere quali elementi devono essere protetti e quali sono i punti deboli che potrebbero essere sfruttati da attori malintenzionati.

Successivamente alla definizione del contesto, il personale preposto alla gestione del rischio informatico procede ad effettuare una valutazione dei potenziali rischi associati alle minacce che potrebbero impattare sui processi identificati nella fase precedente.

Nello specifico, la fase di valutazione del rischio, mira a:

1. identificare gli eventi incerti i cui effetti possono determinare un rischio;
2. analizzare e descrivere i rischi precedentemente identificati e che potrebbero influire negativamente sul raggiungimento degli obiettivi dell'Ente;

3. valutare il rischio attraverso la comparazione dei livelli di rischio risultanti dalla fase precedente, al fine di stabilire dei criteri di accettazione e per quelli estremamente elevati, e quindi inaccettabili, effettuare una prioritizzazione delle minacce da trattare.

Attraverso l'analisi, difatti, vengono determinati i livelli di rischio attuale sulla base dei valori di probabilità di accadimento e dell'impatto. L'analisi del rischio, effettuata mediante un apposito tool di analisi e trattamento del rischio, mira inoltre all'identificazione di una serie di minacce cui il processo oggetto di analisi è esposto e una libreria di controlli di sicurezza, ossia delle contromisure che devono essere implementate al fine di garantire un'efficace gestione e mitigazione dei rischi. Questa analisi permette di classificare i rischi in base alla loro gravità e priorità.

Il Referente, unitamente al Team di supporto e agli specifici responsabili degli affidamenti di interesse analizza, inoltre, anche i rischi informatici connessi all'espletamento delle attività con i fornitori e servizi del Comune di Napoli attraverso puntuali attività di audit, con l'obiettivo di definire un piano per la gestione del rischio informatico che tenga conto dei rischi di cybersecurity afferenti alla catena di approvvigionamento, in conformità con quanto previsto dall'art. 24 del D.lgs. 138/2024.

A seguito dell'identificazione e analisi dei rischi, si passa alla fase di trattamento del rischio, che prevede l'implementazione di opportune azioni di rimedio, in coerenza con i livelli di rischio accettabili prefissati. In particolare, in questa fase viene condotta un'analisi costi/benefici volta ad indirizzare le iniziative e svolgere una stima delle risorse disponibili per contenere i rischi in maniera efficace, efficiente ed adeguata al conseguimento degli obiettivi del Comune di Napoli. Queste azioni possono includere, ad esempio, l'applicazione di best practices di settore o di una serie di indicazioni, aventi quale scopo quello di garantire che le parti coinvolte nel processo oggetto di analisi assicurino determinati livelli di servizio come, ad esempio, aggiornamenti software, configurazioni sicure, attività di formazione del personale, implementazione di sistemi di difesa aggiuntivi, sistemi di rilevamento delle intrusioni e altre tecniche di protezione. La definizione di un Piano di Trattamento del rischio ed il relativo monitoraggio è fondamentale per evitare, mitigare, accettare o trasferire i rischi individuati in fase di analisi, con l'obiettivo finale di prevenire ed evitare di incorrere in eventuali incidenti di sicurezza e rispondere in modo efficace. Inoltre, vengono effettuate revisioni periodiche delle politiche e delle procedure di sicurezza inerenti alle attività di gestione del rischio informatico per assicurarsi che siano sempre aggiornate e adeguate alle nuove minacce insistenti sulle risorse e sui processi dell'Ente. Difatti, la fase finale di monitoraggio del rischio, mira ad assicurare il controllo periodico dei fattori di rischio con l'obiettivo di garantire un presidio costante sulle eventuali modifiche al contesto organizzativo dell'Ente o sulla presenza di nuovi fattori che possano minare la sicurezza delle informazioni e l'adeguatezza dell'intero processo rispetto agli obiettivi strategici e operativi posti dal Comune di Napoli.

5.6 Potenziamento della capacità di gestione dei rischi

Il Comune di Napoli, in conformità con quanto previsto dalla Legge all'art. 8 comma 1 lettera e) e dall'art. 23 e 24 del D.lgs 138/2024, al fine di contrastare le minacce informatiche sempre più frequenti e sofisticate che spesso si sostanziano in attacchi mirati ai dipendenti

coinvolgendo anche i Dirigenti e le alte cariche dell'Ente, pone in essere una serie di attività tese alla sensibilizzazione e formazione del personale. Le attività sono coordinate dal Referente ed eseguite dal Team di supporto, in collaborazione con l'Ufficio Gestione Risorse Umane.

A tal riguardo, il Comune di Napoli stabilisce una serie di iniziative di sicurezza, diversificate per competenza e responsabilità assunte dai singoli dipendenti, come la definizione di appositi Programmi di Formazione che si sostanziano in sessioni formative periodiche inerenti ad argomenti come la gestione delle password, il riconoscimento delle e-mail di phishing, il corretto utilizzo dei dispositivi e la protezione dei dati sensibili. Le sessioni di formazione sono inoltre arricchite da ampie fasi di Q&A in cui vengono poste sessioni di domande e risposte con esperti di sicurezza informatica per affrontare dubbi e perplessità dei dipendenti.

L'Ente, inoltre, nell'ottica di attuare interventi di potenziamento delle capacità di gestione dei rischi informatici da parte dei dipendenti, esegue simulazioni di attacchi, come phishing, ransomware o social engineering, per testare la prontezza dei dipendenti e identificare le aree di miglioramento. Queste simulazioni periodiche, anche erogate in modalità "*tabletop exercises*", sono simulazioni pratiche che coinvolgono in modo interattivo i dipendenti del Comune di Napoli, al fine di discutere e rispondere a scenari ipotetici di incidenti di sicurezza informatica. Queste esercitazioni sono progettate per testare e migliorare la preparazione della popolazione dipendente nella gestione delle crisi e nella risposta agli incidenti di sicurezza.

5.7 Monitoraggio e valutazione delle minacce

Il Comune di Napoli, in conformità con quanto previsto dalla Legge all'art. 8 comma 1 lettera g), al fine di garantire il monitoraggio e la valutazione continua delle minacce alla sicurezza e delle vulnerabilità dei sistemi e infrastruttura dell'Ente, in conformità con le iniziative previste all'interno del Piano Programmatico di Sicurezza Informatica, delle politiche adottate dall'Ente in materia di identificazione e valutazione delle vulnerabilità e di quanto richiesto ai sensi dell'art. 35 del D.lgs 138/2024 in materia di monitoraggio, esegue periodicamente scansioni di tipo VA e di PT.

. Queste attività permettono di identificare e correggere le vulnerabilità presenti nei sistemi informatici, riducendo il rischio di attacchi e migliorando la protezione complessiva dell'infrastruttura IT.

In particolare, nella predetta fase vengono eseguite verifiche tecniche di sicurezza che si suddividono in due principali categorie:

- **Penetration Testing:** è un'attività che mira a verificare la sicurezza dei sistemi IT cercando e sfruttando le vulnerabilità. L'obiettivo è simulare possibili scenari di attacco per vedere come i sistemi reagiscono a tentativi di violazione della riservatezza e dell'integrità dei dati. Questo tipo di test, inoltre, aiuta a capire come un attaccante potrebbe sfruttare le debolezze dei sistemi per accedere a informazioni sensibili o causare danni.
- **Vulnerability Assessment**: si concentra sulla ricerca e raccolta di informazioni riguardanti le debolezze di un sistema IT (scansioni). Queste attività vengono avviate in seguito a diversi input, come l'esigenza palesata dall'Ente, la programmazione

annuale dell'attività di VA o in presenza di eventi di sicurezza verificatisi o, ancora, a valle di avvisi e segnalazioni da parte di soggetti esterni all'Ente (es. AgID, ACN, CSIRT nazionale/regionale), e sono finalizzate a identificare le vulnerabilità che potrebbero causare interruzioni di servizio o permettere intrusioni nei sistemi. L'obiettivo è prevenire attacchi dalla rete e violazioni che potrebbero comportare la perdita, l'abuso o l'esposizione di dati critici per l'Ente.

La fase di identificazione costituisce un passaggio cruciale nella gestione dei rischi, poiché rappresenta il primo passo per mitigare le minacce. È essenziale che questa fase venga eseguita con attenzione, rilevando le caratteristiche specifiche delle vulnerabilità nel contesto tecnologico. Attraverso l'espletamento della fase di cui sopra, il Comune di Napoli assicura il monitoraggio e la valutazione continua delle minacce alla sicurezza e delle vulnerabilità dei sistemi al fine di garantire il loro pronto aggiornamento di sicurezza e proteggere, pertanto, i sistemi IT e la sicurezza dei dati.

Successivamente l'Ente procede alla prioritizzazione delle azioni da applicare alle vulnerabilità scovate, considerando la criticità dell'asset e la "*severity*" della stessa. Questo passaggio risulta essere di fondamentale importanza in quanto indica la celerità e l'urgenza con cui la vulnerabilità dev'essere analizzata e indirizzata, definendo quindi l'ordine con cui le eventuali azioni di rimedio dovranno essere effettuate.

Conclusa questa prima fase di analisi e sintesi dei risultati, l'Ente definisce un piano di rientro. In questa fase, sono definite le azioni necessarie a correggere le vulnerabilità identificate. Il piano serve a stabilire le priorità delle azioni di rimedio, assicurando che le vulnerabilità più gravi e con il maggiore impatto siano affrontate per prime. Il piano, inoltre, specifica le misure correttive da adottare, come aggiornamenti software, modifiche alle configurazioni di sistema, implementazione di patch di sicurezza ecc. Inoltre, assegna le responsabilità per l'implementazione delle misure correttive al Team coinvolto nel processo di sicurezza delle informazioni.

Il Piano di rientro stabilisce anche le tempistiche e le scadenze per l'implementazione delle misure correttive, garantendo che le azioni di rimedio siano eseguite tempestivamente.

5.8 Notifica incidenti di Sicurezza

L'art. 1 della Legge 90/2024 impone ai soggetti individuati, tra cui il Comune di Napoli, di notificare senza ritardo gli incidenti di sicurezza alle autorità competenti. Questo obbligo è fondamentale per garantire una risposta tempestiva ed efficace agli incidenti, minimizzando l'impatto sulle infrastrutture critiche e sui servizi essenziali.
Nello specifico, al fine di ottemperare agli obblighi definiti dalla Legge, il Comune di Napoli segnala e notifica gli incidenti accorsi sulla propria infrastruttura nel rispetto dei tempi e delle modalità previste dalla predetta Legge, tenuto conto della tassonomia degli incidenti dalla stessa prevista all'articolo 1 comma 1.
In tale contesto, in conformità con quanto disposto in materia di obblighi di notifica di incidente dalla predetta Legge e dall'articolo 25 del D.lgs. 138/2024, il Comune di Napoli si premura di **segnalare senza ritardo** e comunque **entro il termine massimo di 24 ore** dal momento in cui ne viene a conoscenza, gli incidenti aventi impatto su reti, sistemi informativi e servizi informatici. L'Ente, inoltre, **entro le 72 ore** decorrenti dal momento in cui viene a conoscenza

dell'incidente, **notifica in modo dettagliato e completo** tutti gli elementi informativi disponibili afferenti all'incidente accorso.

Il Comune effettua la segnalazione e la successiva notifica tramite le apposite procedure disponibili nel sito internet istituzionale dell'Agenzia per la cybersicurezza nazionale (di seguito ACN).

Il Comune, inoltre, si riserva la facoltà di segnalare volontariamente qualsiasi incidente al di fuori dei casi indicati nella tassonomia di cui sopra e in conformità con quanto statuito dalla Legge stessa, nonché di trasmettere segnalazioni volontarie relative a minacce informatiche e quasi-incidenti significativi per la sicurezza cibernetica ai sensi dall'art. 26 del D.lgs. 138/2024. In ogni caso, il Livello 1 di Governo del presente Modello informa la Direzione del Comune su base periodica o, se opportuno, tempestivamente, degli incidenti e delle notifiche di cui agli artt. 25 e 26 del D.lgs. 138/2024.

6. Revisione e Aggiornamento del Documento

Il presente documento è sottoposto ad approvazione formale da parte degli organi direttivi, a garanzia della sua validazione e applicazione ufficiale. È, inoltre, soggetto a riesame periodico, almeno con cadenza annuale o in seguito a eventi rilevanti quali incidenti informatici, cambiamenti organizzativi o variazioni nell'esposizione ai rischi. Il riesame e l'aggiornamento delle politiche e delle procedure di sicurezza sono curati dal Referente per la Cybersicurezza supportato dal Team di Sicurezza Informatica, al fine di garantire il costante allineamento delle misure adottate alle esigenze dell'organizzazione e alla normativa vigente in materia di sicurezza informatica.