Città metropolitana di Milano

Dipartimento Transizione Digitale

Politica di sicurezza informatica

CMM-NIS-POL-00 · versione 1.0

ai sensi del D.lgs. 4 settembre 2024, n. 138 e della Determinazione ACN n. 379907/2025
Approvato con decreto n. 308 del 28/10/2026

SCHEDA DEL DOCUMENTO

Codice	CMM-NIS-POL-00
Titolo	Politica di sicurezza informatica
Versione e data	1.0 del 19/10/2026
Stato	Prima versione, in approvazione.
Perimetro di applicazione	Città metropolitana di Milano – sistemi informativi e di rete, con priorità per i sistemi rilevanti
Requisiti ACN	GV.PO-01 (punti 1-3); GV.PO-02; ambiti a)–p) della Tabella 1 dell'Allegato 1
Allegati	Allegato A – Corrispondenza tra ambiti, misure e documenti; Allegato B – Requisiti di sicurezza per i fornitori ICT
Classificazione	Uso interno

Iter di redazione e approvazione

Fase	Struttura / ruolo	Data e riferimento
Redazione	Dipartimento Transizione Digitale	19/10/2026
Verifica	Servizio Coordinamento sicurezza, service desk e procurement IT (referente CSIRT) e responsabili di ambito	21/10/2026
Istruttoria	Direttrice del Dipartimento Transizione Digitale	23/10/2026
Proposta e parere di regolarità tecnica	Direttore generale	Contenuti nel decreto R.G. n. 308/2026 del 28/10/2026
Approvazione	Direttore generale (organo direttivo), con la sottoscrizione della proposta; Vicesindaco (organo di amministrazione)	Decreto del Sindaco metropolitano R.G. n. 308/2026 del 28/10/2026
Decorrenza	Dalla data di approvazione	

Storico delle revisioni

Versione	Data	Descrizione delle modifiche	Redatto da
1.0	23/10/2026	Prima emissione	Dipartimento Transizione Digitale

INDICE

Definizioni 4
1. Aspetti generali 4
1.1. Introduzione 4
1.2. Obiettivo e ambito di applicazione 4
1.3. Fonti normative 4
2. Principi 5
3. Rapporto con gli altri documenti 5
4. Regole per ambito 5
4.1. Gestione del rischio (ambito a) 5
4.2. Ruoli e responsabilità (ambito b) 6
4.3. Affidabilità delle risorse umane (ambito c) 6
4.4. Conformità e audit di sicurezza (ambito d) 6
4.5. Catena di approvvigionamento (ambito e) 6
4.6. Gestione degli asset (ambito f) 6
4.7. Gestione delle vulnerabilità (ambito g) 7
4.8. Continuità operativa, ripristino e crisi (ambito h) 7
4.9. Identità digitali, autenticazione e controllo degli accessi (ambito i) 7
4.10. Sicurezza fisica (ambito j) 7
4.11. Formazione e consapevolezza (ambito k) 7
4.12. Sicurezza dei dati (ambito l) 8
4.13. Sviluppo, configurazione, manutenzione e dismissione (ambito m) 8
4.14. Protezione delle reti e delle comunicazioni (ambito n) 8
4.15. Monitoraggio degli eventi di sicurezza (ambito o) 8
4.16. Gestione degli incidenti, risposta e ripristino (ambito p) 8
5. Eccezioni 9
6. Approvazione e comunicazione 9
7. Formazione e sensibilizzazione 9
8. Violazioni 9
9. Revisione e aggiornamento 9
Allegato A – Corrispondenza tra ambiti, misure e documenti 9
Allegato B – Requisiti di sicurezza per i fornitori ICT 10
B.1 Classificazione dei fornitori 10
B.2 Requisiti contrattuali 10

DEFINIZIONI

Termine	Definizione
Sistemi rilevanti	Sistemi informativi e di rete individuati dall'ente ai sensi della misura GV.OC-04, elencati nell'Allegato A del documento CMM-NIS-PIA-a1.
DTD	Dipartimento Transizione Digitale.
Servizio Coordinamento sicurezza	Servizio Coordinamento sicurezza, service desk e procurement IT del DTD.
Organi	Organi di amministrazione e direttivi ai fini NIS individuati con decreto R.G. 128/2025: Vicesindaco e Direttore generale.
ACN / CSIRT Italia	Agenzia per la Cybersicurezza Nazionale e il suo Computer Security Incident Response Team, destinatario delle notifiche degli incidenti significativi.
Politica	Insieme di principi e regole approvati dagli organi, che orientano procedure e piani.
Procedura	Documento operativo che descrive come si attua una regola, chi fa cosa e con quali strumenti.
Fornitore rilevante (Tier 1)	Fornitore classificato ad alta criticità secondo i criteri dell'Allegato B.

1. ASPETTI GENERALI

1.1. INTRODUZIONE

La politica stabilisce i principi e le regole con cui la Città metropolitana di Milano protegge i propri sistemi informativi e di rete e i dati che tratta. Copre i sedici ambiti indicati dalla Tabella 1 dell'Allegato 1 alla Determinazione ACN n. 379907/2025 ed è il riferimento per tutti i piani e le procedure di sicurezza.[1]

1.2. OBIETTIVO E AMBITO DI APPLICAZIONE

Si applica a tutti i sistemi informativi e di rete dell'ente, in cloud o nelle sedi, con priorità per i sistemi rilevanti; a tutto il personale, agli amministratori, ai collaboratori, agli stagisti e ai volontari del servizio civile; ai fornitori che accedono ai sistemi o ai dati dell'ente, per i quali le regole sono rese vincolanti tramite i contratti.

1.3. FONTI NORMATIVE

- D.lgs. 4 settembre 2024, n. 138 (decreto NIS), in particolare artt. 23, 24 e 25.
- Determinazione ACN n. 379907/2025, Allegato 1 – misure di sicurezza di base per i soggetti importanti – e Allegato 3 – incidenti significativi di base.
- ACN, Linee guida NIS – Specifiche di base – Guida alla lettura.
- Legge 28 giugno 2024, n. 90 (disposizioni in materia di rafforzamento della cybersicurezza nazionale).
- Regolamento (UE) 2016/679 (GDPR).
- D.lgs. 7 marzo 2005, n. 82 (Codice dell'amministrazione digitale).
- D.lgs. 31 marzo 2023, n. 36 (Codice dei contratti pubblici).
- Legge 20 maggio 1970, n. 300, art. 4 (impianti e strumenti di controllo).

[1] Requisito GV.PO-01, punti 1 e 2: politiche di sicurezza per gli ambiti della Tabella 1.

2. PRINCIPI

- **Responsabilità degli organi:** gli organi approvano la politica e ne sovrintendono l'attuazione; la Direttrice del DTD ne cura l'applicazione.
- **Proporzionalità al rischio:** le misure sono commisurate al rischio valutato con il metodo di CMM-NIS-PIA-a1.
- **Minimo privilegio:** ognuno accede solo a ciò che serve per il proprio lavoro.
- **Sicurezza fin dalla progettazione:** il DTD è coinvolto fin dall'inizio in ogni acquisto o progetto ICT, anche dei Settori.
- **Nessun sistema fuori dall'inventario:** ogni sistema, servizio cloud o fornitore ICT è noto al DTD.
- **Segnalare sempre:** chiunque noti un'anomalia la segnala subito; nessuno è sanzionato per una segnalazione in buona fede.
- **Tracciabilità:** decisioni, eccezioni e verifiche sono documentate.

3. RAPPORTO CON GLI ALTRI DOCUMENTI

La politica è attuata dai piani del pacchetto NIS e dalle procedure indicate nell'Allegato A. Restano in vigore, per quanto compatibili, e sono allineati alla politica al primo riesame:

- il **Disciplinare per l'utilizzo dei servizi informatici** e di comunicazione telematica, approvato con decreto del Sindaco metropolitano R.G. 230/2024 del 24/09/2024, che contiene le regole d'uso degli strumenti ICT rivolte al personale. Al primo riesame va allineato alla presente politica, in particolare estendendo a qualunque incidente di sicurezza l'obbligo di segnalazione al DTD, oggi previsto per gli incidenti che possono comportare una violazione di dati personali;
- il documento **Misure minime di sicurezza ICT**, versione 1 del 28/12/2017, adottato ai sensi della circolare AgID n. 2/2017.[2] Molti impegni assunti allora (politiche per configurazioni standard, aggiornamenti, vulnerabilità, utenze amministrative, accessi remoti) trovano attuazione nella presente politica e nei documenti del pacchetto NIS. Il documento non è stato più aggiornato: il suo aggiornamento è previsto entro giugno 2027, in coordinamento con il Manuale di gestione documentale.

4. REGOLE PER AMBITO

4.1. GESTIONE DEL RISCHIO (AMBITO A)

- L'ente mantiene l'elenco dei sistemi rilevanti, collegato ai servizi categorizzati sul portale ACN, e lo aggiorna a ogni variazione significativa.
- Il rischio è valutato almeno ogni due anni e dopo incidenti significativi o cambiamenti rilevanti, anche con riferimento ai fornitori.
- Ogni rischio non accettabile ha un trattamento con responsabile e data; i rischi residui sono accettati in modo motivato dai soggetti indicati in CMM-NIS-PIA-a1.

Documenti attuativi: CMM-NIS-PIA-a1; CMM-NIS-PIA-a2.[3]

[2] Il documento è riservato e non è allegato alla presente politica.
[3] Requisiti GV.OC-04, GV.RM-03, ID.RA-05, ID.RA-06.

4.2. Ruoli e responsabilità (ambito b)

- Ruoli, responsabilità e sostituti sono definiti in CMM-NIS-POL-b e riesaminati almeno ogni due anni.
- L'elenco del personale con ruoli di sicurezza è mantenuto aggiornato insieme ai ruoli sul portale ACN.

Documenti attuativi: CMM-NIS-POL-b.[4]

4.3. Affidabilità delle risorse umane (ambito c)

- Il personale con accesso privilegiato ai sistemi rilevanti, interno o dei fornitori, è individuato nominativamente dopo una valutazione di esperienza, capacità e affidabilità.
- Gli amministratori di sistema sono nominati con atto individuale; l'elenco è riesaminato almeno una volta l'anno.

Documenti attuativi: CMM-NIS-POL-b, capitolo 5.[5]

4.4. Conformità e audit di sicurezza (ambito d)

- La politica è riesaminata almeno una volta l'anno e quando cambiano norme, rischi o organizzazione.
- Lo stato di attuazione è seguito con il Piano di adeguamento; la Direttrice riferisce agli organi ogni sei mesi.

Documenti attuativi: CMM-NIS-PIA-d.[6]

4.5. Catena di approvvigionamento (ambito e)

- Per ogni acquisto ICT con possibili impatti sui sistemi il RUP coinvolge il DTD dalla fase di progettazione, anche con convenzioni o centrali di committenza.
- Il fornitore è classificato Tier 1 o Tier 2 secondo l'Allegato B; bandi, contratti e convenzioni includono i requisiti di sicurezza dell'Allegato B, salvo motivate e documentate ragioni, nel qual caso il rischio è trattato con misure compensative.
- Il Registro dei fornitori e dei contratti ICT è aggiornato a ogni affidamento, rinnovo o cessazione; per i fornitori Tier 1 il rischio è valutato e la conformità verificata almeno una volta l'anno.

Documenti attuativi: Registro dei fornitori e dei contratti ICT; Allegato B.[7]

4.6. Gestione degli asset (ambito f)

- L'ente mantiene inventari aggiornati di apparati (compresi rete, dispositivi mobili e IoT), software e applicazioni (compresi API e software open source) e servizi dei fornitori, compresi quelli cloud.
- Ogni nuovo sistema o servizio è registrato prima della messa in produzione, con il relativo responsabile.

Documenti attuativi: catalogo delle applicazioni; inventari di rete e postazioni; Registro fornitori.[8]

[4]Requisiti GV.RR-02.
[5]Requisiti GV.RR-04.
[6]Requisiti GV.PO-01, GV.PO-02, ID.IM-01.
[7]Requisiti GV.SC-01, GV.SC-02, GV.SC-04, GV.SC-05, GV.SC-07.
[8]Requisiti ID.AM-01, ID.AM-02, ID.AM-04.

4.7. GESTIONE DELLE VULNERABILITÀ (AMBITO G)

- Le segnalazioni del CSIRT Italia e delle altre fonti sono gestite con un flusso unico, tracciato e assegnato.
- Le vulnerabilità sono risolte nei tempi fissati per gravità, oppure mitigate o accettate in modo motivato.
- Almeno una volta l'anno si svolge un penetration test sui sistemi rilevanti.

Documenti attuativi: CMM-NIS-PIA-g.[9]

4.8. CONTINUITÀ OPERATIVA, RIPRISTINO E CRISI (AMBITO H)

- Per i sistemi rilevanti l'ente mantiene piani di continuità, di ripristino e di gestione delle crisi, approvati e riesaminati almeno ogni due anni, e li verifica con test periodici.
- Gli obiettivi di ripristino sono definiti dai responsabili dei servizi e verificati con i fornitori.

Documenti attuativi: CMM-NIS-PIA-h.[10]

4.9. IDENTITÀ DIGITALI, AUTENTICAZIONE E CONTROLLO DEGLI ACCESSI (AMBITO I)

- Le utenze sono censite, individuali e approvate; le utenze tecniche hanno un responsabile.
- Le utenze sono create, modificate e revocate su comunicazione tempestiva delle strutture del personale, compresi stagisti e servizio civile, e verificate almeno una volta l'anno.
- Le utenze amministrative sono distinte da quelle di uso quotidiano.
- L'autenticazione a più fattori è obbligatoria per l'accesso remoto e per i servizi cloud dell'ente; per i sistemi rilevanti è adottata in base al rischio.
- Gli accessi remoti, anche dei fornitori, avvengono solo tramite la VPN dell'ente; per ogni fornitore il referente interno indica sistemi e permessi; l'elenco dei sistemi accessibili da remoto è mantenuto aggiornato.

Documenti attuativi: procedura di gestione delle utenze da redigere; configurazioni VPN e firewall.[11]

4.10. SICUREZZA FISICA (AMBITO J)

- L'accesso ai locali tecnici e agli apparati dei sistemi rilevanti è consentito al solo personale autorizzato ed è registrato.
- Dove gli armadi di rete non possono essere protetti fisicamente, il rischio di accesso non autorizzato alla rete è compensato dal NAC; il rischio di danneggiamento fisico degli apparati resta e va trattato nel piano di trattamento del rischio.

Documenti attuativi: procedura di accesso ai locali tecnici da redigere.[12]

4.11. FORMAZIONE E CONSAPEVOLEZZA (AMBITO K)

- Tutto il personale riceve formazione sulla sicurezza informatica; per organi, dirigenti, referente CSIRT, sostituti e amministratori di sistema sono previsti percorsi specifici.
- La partecipazione è registrata e verificata.

Documenti attuativi: CMM-NIS-PIA-k.[13]

[9] Requisiti ID.RA-01, ID.RA-08.
[10] Requisiti ID.IM-04.
[11] Requisiti PR.AA-01, PR.AA-03, PR.AA-05, PR.IR-01.
[12] Requisiti PR.AA-06.
[13] Requisiti PR.AT-01.

4.12. SICUREZZA DEI DATI (AMBITO L)

- I dati su dispositivi portatili e supporti rimovibili sono cifrati; l'esecuzione automatica dei supporti è disabilitata e i supporti sono analizzati prima dell'uso.
- Le comunicazioni da e verso l'esterno dei sistemi rilevanti usano protocolli cifrati sicuri.
- Dati e configurazioni sono salvati periodicamente in coerenza con i piani di continuità; per i sistemi rilevanti esiste una copia offline o non modificabile.
- Nessun server è messo in produzione senza backup attivo.

Documenti attuativi: CMM-NIS-PIA-h, capitolo sul backup.[14]

4.13. SVILUPPO, CONFIGURAZIONE, MANUTENZIONE E DISMISSIONE (AMBITO M)

- Si installano solo software e sistemi operativi con aggiornamenti di sicurezza disponibili; le eccezioni sono motivate, compensate e hanno una data di dismissione.
- Gli aggiornamenti di sicurezza sono installati senza ingiustificato ritardo.
- Gli accessi remoti e privilegiati sono registrati; per i sistemi rilevanti i log sono raccolti in modo sicuro e possibilmente centralizzato, con tempi di conservazione definiti.
- Lo sviluppo del software segue pratiche di sviluppo sicuro, anche per i fornitori.

Documenti attuativi: CMM-NIS-PIA-g; linee guida di sviluppo sicuro da redigere.[15]

4.14. PROTEZIONE DELLE RETI E DELLE COMUNICAZIONI (AMBITO N)

- I firewall sono mantenuti aggiornati e configurati in modo adeguato; le regole sono documentate e riesaminate.
- La rete è progressivamente segmentata; l'accesso alla LAN è consentito solo a dispositivi e utenti dell'ente.

Documenti attuativi: configurazioni di rete; progetto rete.[16]

4.15. MONITORAGGIO DEGLI EVENTI DI SICUREZZA (AMBITO O)

- Per i sistemi rilevanti l'ente dispone di strumenti per rilevare tempestivamente gli incidenti significativi e definisce i livelli di servizio attesi.
- Postazioni e server sono protetti da sistemi aggiornati di rilevamento del codice malevolo.

Documenti attuativi: CMM-NIS-PIA-p (livelli di servizio attesi).[17]

4.16. GESTIONE DEGLI INCIDENTI, RISPOSTA E RIPRISTINO (AMBITO P)

- Gli incidenti sono gestiti da un gruppo secondo il piano dedicato; gli incidenti significativi sono notificati al CSIRT Italia nei tempi dell'art. 25 del decreto NIS.
- Tutte le strutture e i fornitori segnalano subito al DTD qualunque incidente sui sistemi che gestiscono.
- L'ente informa utenti e pubblico quando opportuno o richiesto dall'ACN e ripristina i sistemi con procedure documentate.

Documenti attuativi: CMM-NIS-PIA-p.[18]

[14] Requisiti PR.DS-01, PR.DS-02, PR.DS-11.
[15] Requisiti PR.PS-02, PR.PS-04, PR.PS-06.
[16] Requisiti PR.IR-01.
[17] Requisiti DE.CM-01, DE.CM-09.
[18] Requisiti RS.MA-01, RS.CO-02, RC.RP-01.

5. ECCEZIONI

Una regola può non essere applicata solo per motivate ragioni tecniche o normative, documentate dal responsabile di ambito e approvate dalla Direttrice, con misure compensative e data di superamento. Le eccezioni sono registrate nel registro unico dei rischi e delle vulnerabilità (ALL-a1).

6. APPROVAZIONE E COMUNICAZIONE

La politica è approvata dagli organi di amministrazione e direttivi.[19] È pubblicata nella intranet, comunicata a tutte le strutture e richiamata nei contratti con i fornitori. Le regole che riguardano la registrazione e il monitoraggio delle attività del personale sono applicate nel rispetto dell'art. 4 della legge 300/1970.

7. FORMAZIONE E SENSIBILIZZAZIONE

Il personale con ruoli nell'attuazione del presente documento riceve una formazione specifica sui suoi contenuti, secondo il Piano di formazione in materia di sicurezza informatica (CMM-NIS-PIA-k).

8. VIOLAZIONI

La violazione delle disposizioni del presente documento da parte del personale è valutata secondo il Codice di comportamento dell'ente e le norme disciplinari vigenti; per i fornitori, secondo le clausole contrattuali.

9. REVISIONE E AGGIORNAMENTO

La politica è riesaminata almeno una volta l'anno e comunque in caso di incidenti significativi, variazioni organizzative, mutamenti dell'esposizione alle minacce o modifiche normative.[20] Il riesame è curato dal Servizio Coordinamento sicurezza e approvato dalla Direttrice; le modifiche sostanziali sono sottoposte agli organi.

ALLEGATO A – CORRISPONDENZA TRA AMBITI, MISURE E DOCUMENTI

Ambito	Misure ACN	Documento attuativo	Stato al 31/10/2026
a) Gestione del rischio	GV.OC-04, GV.RM-03, ID.RA-05, ID.RA-06	CMM-NIS-PIA-a1, PIA-a2	Approvato
b) Ruoli e responsabilità	GV.RR-02	CMM-NIS-POL-b	Approvato
c) Affidabilità risorse umane	GV.RR-04	CMM-NIS-POL-b	Approvato; nomine in corso
d) Conformità e audit	GV.PO-01, GV.PO-02, ID.IM-01	CMM-NIS-POL-00, PIA-d	Approvato
e) Catena di approvvigionamento	GV.SC-01, -02, -04, -05, -07	Allegato B; Registro fornitori	Approvato; clausole ai rinnovi
f) Asset	ID.AM-01, -02, -04	Inventari	In corso
g) Vulnerabilità	ID.RA-01, ID.RA-08	CMM-NIS-PIA-g	Approvato

[19] Requisito GV.PO-01, punto 3.
[20] Requisito GV.PO-02.

Ambito	Misure ACN	Documento attuativo	Stato al 31/10/2026
h) Continuità e crisi	ID.IM-04	CMM-NIS-PIA-h	Approvato
i) Identità e accessi	PR.AA-01, -03, -05; PR.IR-01	Procedura utenze	Da redigere (2027)
j) Sicurezza fisica	PR.AA-06	Procedura locali tecnici	Da redigere (2027)
k) Formazione	PR.AT-01	CMM-NIS-PIA-k	Approvato
l) Sicurezza dei dati	PR.DS-01, -02, -11	CMM-NIS-PIA-h	Approvato
m) Sviluppo e manutenzione	PR.PS-02, -04, -06	CMM-NIS-PIA-g; linee guida	Parziale
n) Reti	PR.IR-01	Configurazioni	Parziale
o) Monitoraggio	DE.CM-01, DE.CM-09	CMM-NIS-PIA-p	Approvato; SIEM da attivare
p) Incidenti	RS.MA-01, RS.CO-02, RC.RP-01	CMM-NIS-PIA-p	Approvato

ALLEGATO B – REQUISITI DI SICUREZZA PER I FORNITORI ICT

B.1 Classificazione dei fornitori

Il fornitore è classificato **Tier 1 (alta criticità)** se ricorre anche uno solo dei criteri seguenti; altrimenti è **Tier 2 (standard)**. La classificazione è riportata nel Registro dei fornitori e dei contratti ICT.

Criterio	Tier 1 – alta criticità	Tier 2 – standard
Accesso ai sistemi	Accesso diretto, remoto o fisico, a sistemi rilevanti, identità, rete o dati riservati	Accesso limitato a sistemi non rilevanti o nessun accesso
Impatto sulla continuità	Il fermo blocca un servizio rilevante (es. protocollo, firma, rete, posta)	Disservizi parziali recuperabili senza impatto sui servizi rilevanti
Dati trattati	Dati personali in quantità o dati riservati	Dati non personali o in quantità limitata
Sostituibilità	Fornitore unico o sostituibile in più di sei mesi	Sostituibile con procedura ordinaria
Ruolo nella catena	Gestisce l'infrastruttura per conto dell'ente o è subfornitore di un Tier 1	Fornitore autonomo

B.2 Requisiti contrattuali

Requisito	Tier 1	Tier 2
Notifica degli incidenti all'ente: pre-notifica entro 12 ore dalla conoscenza, notifica entro 48 ore, relazione finale entro 20 giorni; anche senza dati personali	Obbligatorio	Obbligatorio
Referente per la sicurezza e contatto raggiungibile fuori orario	Obbligatorio	Raccomandato
Elenco nominativo del personale con accessi; nomina ad amministratore di sistema; accesso solo via VPN dell'ente con MFA; revoca a fine incarico	Obbligatorio	Obbligatorio se ha accessi
Livelli di servizio di intervento e ripristino, con RTO e RPO	Obbligatorio	Raccomandato
Backup con copia offline o non modificabile; test di ripristino almeno annuale con verbale	Obbligatorio se gestisce sistemi o dati	—
Aggiornamenti di sicurezza nei tempi di CMM-NIS-PIA-g; nessun componente fuori supporto senza accordo	Obbligatorio	Obbligatorio
Conservazione dei log di accesso e sicurezza per almeno 12 mesi e messa a disposizione	Obbligatorio	—

Requisito	Tier 1	Tier 2
Diritto di verifica (audit) dell'ente o di un terzo incaricato	Obbligatorio	Raccomandato
Autorizzazione preventiva dei subfornitori e trasferimento degli stessi obblighi	Obbligatorio	Obbligatorio
Restituzione e cancellazione sicura dei dati a fine contratto; supporto al subentro	Obbligatorio	Obbligatorio

Per i contratti in essere, non modificabili prima del rinnovo, il DTD chiede ai fornitori Tier 1 un impegno scritto alla notifica degli incidenti; le prime occasioni di inserimento delle clausole sono i rinnovi di InfoCert (31/12/2026), CSI Piemonte (2027-2028) e il nuovo contratto Consip alla scadenza dell'attuale SGM2 (31/08/2028).