DELIBERAZIONE DELLA GIUNTA REGIONALE 4 agosto 2026, n. 1107

Approvazione dei documenti attuativi regionali in materia di gestione degli eventi e degli incidenti di sicurezza informatica, ai fini dell'attuazione del decreto legislativo 4 settembre 2024, n. 138 e della legge 28 giugno 2024, n. 90

GIUNTA REGIONALE

VISTI:

- gli artt. 4, 5 e 6 della L.R. 4 febbraio 1997, n.7;
- la Deliberazione della Giunta Regionale n. 3261 del 28 luglio 1998;
- gli art. 4 e 16 del D. Lgs n. 165 del 30.03.2001 e ss.mm.ii;
- gli artt. 43 e 44 dello Statuto della Regione Puglia;
- il Decreto del Presidente della Giunta Regionale 22 gennaio 2021, n.22 e ss.mm.ii recante l'Atto di Alta Organizzazione "M.A.I.A. 2.0";
- il Regolamento interno di questa Giunta;

VISTO il documento istruttorio della Sezione Cloud, Cybersecurity e Infrastrutture Tecnologiche concernente l'argomento in oggetto, e la conseguente proposta dell'Assessore al Bilancio e Personale, Sebastiano Giuseppe Leo.

PRESO ATTO

a) delle sottoscrizioni dei responsabili delle strutture amministrative competenti, ai fini dell'attestazione della regolarità amministrativa dell'attività istruttoria e della proposta, ai sensi dell'art. *5,* co. 8 delle Linee guida sul "Sistema dei controlli interni della Regione Puglia", adottate *con D.G.R.* 7 *ottobre 2025, n. 1397;*

b) della dichiarazione del Direttore del Dipartimento per la Transizione Digitale, in merito a eventuali osservazioni sulla proposta di deliberazione, ai sensi degli artt. 18 e 20 del Decreto del Presidente della Giunta regionale 22 gennaio 2021, n. 22 e ss.mm.ii.;

Con voto favorevole espresso all'unanimità dei presenti e per le motivazioni contenute nel documento istruttorio che è parte integrante e sostanziale della presente deliberazione.

DELIBERA

1. di approvare i documenti attuativi regionali in materia di gestione degli eventi e degli incidenti di sicurezza informatica, allegati alla presente deliberazione quali parti integranti e sostanziali, come di seguito indicati:
    - Allegato A - Procedura di gestione degli eventi e degli incidenti di sicurezza informatica relativi alla Regione Puglia;
    - Allegato B - Registro incidenti della Regione Puglia.
2. di dare atto che i documenti di cui al precedente punto costituiscono il quadro attuativo regionale in materia di gestione degli eventi e degli incidenti di sicurezza informatica, in coerenza con il modello strategico regionale della cybersecurity e con la disciplina nazionale ed europea di settore;
3. di demandare al Dipartimento per la Transizione Digitale il coordinamento dell'attuazione dei documenti

approvati con il presente provvedimento, nell'ambito delle funzioni di governance regionale della cybersecurity, ferme restando, nei singoli documenti allegati, le attribuzioni del Referente per la cybersecurity per i profili di competenza;

4. di demandare alla Sezione Cloud, Cybersecurity e Infrastrutture Tecnologiche l'adozione dei conseguenti atti organizzativi e gestionali di competenza, nonché l'attuazione delle misure necessarie a dare esecuzione ai documenti approvati con il presente provvedimento;

5. di stabilire che eventuali modifiche ed integrazioni non sostanziali dei documenti approvati con il presente provvedimento, che si rendano necessarie e/o opportune ai fini dell'aggiornamento operativo, organizzativo o normativo, siano adottate con atto della Dirigente della Sezione Cloud, Cybersecurity e Infrastrutture Tecnologiche, nel rispetto degli indirizzi del Dipartimento per la Transizione Digitale e ferme restando, nei singoli documenti allegati, le attribuzioni del Referente per la cybersecurity per i profili di competenza;

6. di dare atto che restano ferme, per eventuali modifiche sostanziali dei documenti approvati con il presente provvedimento, le competenze degli organi regionali secondo il vigente assetto organizzativo e ordinamentale;

7. di notificare il presente provvedimento, a cura del Dipartimento per la Transizione Digitale, ai soggetti interessati;

8. di demandare al Dipartimento per la Transizione Digitale e alla Sezione Cloud, Cybersecurity e Infrastrutture Tecnologiche gli adempimenti amministrativi di rispettiva competenza per l'esatta esecuzione del presente provvedimento;

9. di disporre la pubblicazione del presente provvedimento ad eccezione degli allegati A e B nel Bollettino Ufficiale della Regione Puglia;

10. di dare atto che il presente provvedimento è soggetto a pubblicazione ai sensi dell'art. 23 del D. Lgs 14 marzo 2013, n. 33, ad eccezione degli allegati A e B, sul sito istituzionale della Regione Puglia, nella sezione "Amministrazione Trasparente", sottosezione "Provvedimenti".

Il Segretario Generale della Giunta
NICOLA PALADINO

Il Presidente della Giunta
ANTONIO DECARO

DOCUMENTO ISTRUTTORIO

OGGETTO: **Approvazione dei documenti attuativi regionali in materia di gestione degli eventi e degli incidenti di sicurezza informatica, ai fini dell'attuazione del decreto legislativo 4 settembre 2024, n. 138 e della legge 28 giugno 2024, n. 90.**

Visti:

- il D. Lgs. n. 82 del 7 marzo 2005, "Codice dell'amministrazione digitale";
- il Regolamento (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, che abroga la Direttiva 95/46/CE (Regolamento generale sulla protezione dei dati), e il D. Lgs. n. 196/2003 e ss.mm.ii.;
- la Legge n. 241 del 7 agosto 1990 e ss.mm.ii., "Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi";
- la D.G.R. n. 1974 del 7 dicembre 2020, con la quale la Giunta regionale ha adottato la Macrostruttura del Modello organizzativo denominato "M.A.I.A. 2.0", quale atto di alta organizzazione che disciplina l'organizzazione amministrativa della Presidenza e della Giunta Regionale;
- il D.P.G.R. n. 22 del 22 gennaio 2021, pubblicato sul BURP n. 15 del 28.01.2021, recante l'adozione dell'Atto di Alta Organizzazione "Modello Organizzativo M.A.I.A. 2.0", e ss.mm.ii.;
- la D.G.R. n. 282 del 14 marzo 2024, avente ad oggetto "Modifiche ed integrazioni alla deliberazione di Giunta Regionale n. 1974 del 7 dicembre 2020 e ss.mm.ii. – Nuove istituzioni, rimodulazioni e soppressioni di strutture dirigenziali", con cui è stato istituito il Dipartimento per la Transizione Digitale, comprendente, tra le altre, la Sezione Cloud, Cybersecurity e Infrastrutture Tecnologiche;
- la D.G.R. n. 477 del 15 aprile 2024, con cui la Giunta regionale ha aggiornato le funzioni delle Sezioni del Dipartimento in attuazione della D.G.R. n. 282/2024, dettagliando, in particolare, la declaratoria della Sezione Cloud, Cybersecurity e Infrastrutture Tecnologiche;
- la D.G.R. n. 1872 del 23 dicembre 2024, con cui la Giunta regionale ha conferito l'incarico di Direttore del Dipartimento per la Transizione Digitale all'Ing. Cosimo Elefante;
- la D.G.R. n. 51 del 29 gennaio 2025, con cui la Giunta regionale ha nominato Responsabile per la Transizione al Digitale della Regione Puglia il Direttore pro tempore del Dipartimento per la Transizione Digitale, Ing. Cosimo Elefante;
- la D.G.R. n. 248 del 4 marzo 2025, con cui la Giunta regionale ha conferito l'incarico di direzione della Sezione Cloud, Cybersecurity e Infrastrutture Tecnologiche alla dott.ssa Angela Guerra;
- la D.G.R. n. 1219 del 22 luglio 2021, avente ad oggetto "Riorganizzazione digitale dell'amministrazione regionale - Linee di indirizzo";
- la D.G.R. n. 791 del 30 giugno 2022, con cui la Giunta regionale ha adottato il "Piano triennale di Riorganizzazione Digitale della Regione Puglia 2022-2024" e ss.mm.ii.;
- la D.G.R. n. 663 del 16 maggio 2023, avente ad oggetto "Linee di indirizzo per le infrastrutture tecnologiche digitali regionali";
- la D.G.R. n. 1760 del 30 novembre 2023, avente ad oggetto "P.R. Puglia 2021-2027 - Azione 1.8 - Sub Azione 1.8.2 'Interventi per la transizione digitale della PA' e Fondo Sanitario Regionale - Atto di indirizzo per l'avvio degli interventi. Variazione al bilancio di previsione 2023 e pluriennale 2023-2025 ai sensi dell'art. 51 comma 2 del D. Lgs. n. 118/2011 e ss.mm.ii.";
- la Determinazione Dirigenziale del Dirigente del Servizio Tecnico e Transizione Digitale n. 7 del 7 dicembre 2023, avente ad oggetto "Piano di Potenziamento della Cybersecurity della Regione Puglia. Approvazione Piano Operativo e affidamento in house a InnovaPuglia S.p.A.";
- la Legge n. 90 del 28 giugno 2024, recante "Disposizioni in materia di rafforzamento della cybersecurity nazionale e di reati informatici";
- il D. Lgs. n. 138 del 4 settembre 2024, recante attuazione della Direttiva (UE) 2022/2555 (NIS2);

- la D.G.R. n. 1793 del 16 dicembre 2024, avente ad oggetto indirizzi sulla cybersecurity regionale, individuazione della struttura e del referente per la cybersecurity e designazione del Punto di Contatto soggetto NIS;
- la Determinazione Dirigenziale del Dirigente del Servizio Tecnico e Transizione Digitale n. 8 del 30 dicembre 2024, avente ad oggetto l'approvazione della documentazione CSIRT Regione Puglia e delle relative indicazioni operative;
- la Determinazione del Direttore generale dell'ACN n. 136430 del 12 aprile 2025, con cui la Regione Puglia è stata individuata quale soggetto importante ai sensi del D. Lgs. n. 138/2024;
- la Determinazione del Direttore generale dell'ACN n. 379907/2025, applicabile dal 15 gennaio 2026, recante obblighi di base, misure di sicurezza di base per soggetti essenziali e importanti e tassonomie degli incidenti significativi;
- la Determinazione del Direttore generale dell'ACN n. 379887/2025, applicabile dal 31 dicembre 2025, concernente le modalità organizzative e operative per l'utilizzo del Portale ACN e dei servizi NIS;
- la D.G.R. n. 1258 dell'11 agosto 2025, recante individuazione del Sostituto Punto di Contatto soggetto NIS e aggiornamento delle strutture regionali;
- la D.G.R. n. 1480 del 7 ottobre 2025, recante approvazione del Modello Strategico della Cybersecurity Regionale;
- l'Atto Dirigenziale n. 32 del 12 dicembre 2025, recante aggiornamento del Piano Operativo "Piano di potenziamento della Cybersecurity della Regione Puglia".

Viste altresì:

- la D.G.R. n. 1466 del 15 settembre 2021, recante l'approvazione della Strategia regionale per la parità di genere, denominata "Agenda di Genere";
- la D.G.R. n. 1295 del 26 settembre 2024, recante "Valutazione di Impatto di Genere (VIG). Approvazione indirizzi metodologico-operativi e avvio fase strutturale".

Premesso che:

- con la D.G.R. n. 791 del 30 giugno 2022, la Giunta Regionale ha adottato il "Piano triennale di Riorganizzazione Digitale della Regione Puglia 2022-2024" e ha stabilito, tra l'altro, di affidare la governance del Piano Triennale di Riorganizzazione Digitale al Responsabile per la Transizione al Digitale, coinvolgendo i Dirigenti delle strutture interessate e la società in house InnovaPuglia S.p.A.;
- con il Piano triennale di Riorganizzazione Digitale 2022-2024 e con i relativi aggiornamenti approvati, l'Amministrazione regionale ha delineato il proprio quadro strategico per la transizione al digitale, prevedendo, tra gli altri, l'obiettivo realizzativo concernente il rafforzamento delle infrastrutture di cybersecurity e networking;
- nell'ambito del predetto percorso, è stato previsto il Piano di Potenziamento della Cybersecurity della Regione Puglia, finalizzato al rafforzamento della postura di sicurezza del sistema regionale, alla definizione di strumenti organizzativi e operativi uniformi e al consolidamento della capacità di prevenzione, gestione e risposta agli eventi e incidenti di sicurezza informatica;
- il Modello Strategico della Cybersecurity Regionale, approvato con D.G.R. n. 1480/2025, costituisce il quadro di riferimento per la governance regionale della cybersecurity e per l'adozione dei documenti attuativi regionali necessari a disciplinare in modo uniforme i processi di gestione degli eventi e incidenti di sicurezza informatica e la correlata programmazione formativa in materia di cybersecurity;
- tra i documenti attuativi del predetto modello rientrano, in particolare, la procedura di gestione degli eventi e degli incidenti di sicurezza informatica e il registro degli incidenti.

Considerato che:

- con Determinazione Dirigenziale n. 7 del 7 dicembre 2023 è stato approvato il Piano Operativo del "Piano di Potenziamento della Cybersecurity della Regione Puglia", affidandone l'esecuzione ad InnovaPuglia S.p.A., con l'individuazione, tra i driver di intervento, del governo omogeneo della cybersecurity, della partecipazione collaborativa, del sistema di gestione degli incidenti e delle crisi, della gestione continua delle minacce e della cultura della sicurezza;

- la Legge n. 90/2024, all'art. 8, ha previsto per le amministrazioni regionali l'obbligo di individuare una struttura competente in materia di cybersecurity, cui affidare, tra l'altro, lo sviluppo delle politiche e delle procedure di sicurezza delle informazioni, la pianificazione degli interventi di potenziamento delle capacità di gestione dei rischi informatici e la programmazione della formazione;
- con D.G.R. n. 1793/2024 la Giunta regionale ha individuato nell'Ufficio per la Transizione al Digitale la struttura presso la quale opera il referente per la cybersecurity, individuando nel Responsabile per la Transizione al Digitale il referente per la cybersecurity e affidandogli il coordinamento, la governance e la definizione degli indirizzi strategici in materia di cybersecurity;
- con la D.G.R. n. 1258/2025 la Giunta regionale ha designato il Sostituto Punto di Contatto soggetto NIS e ha demandato al Direttore del Dipartimento per la Transizione Digitale, in collaborazione con la Sezione Cloud, Cybersecurity e Infrastrutture Tecnologiche e con InnovaPuglia S.p.A., il coordinamento, la pianificazione, la progettazione e l'implementazione delle politiche di sicurezza informatica ai sensi dell'art. 23 del D. Lgs. n. 138/2024, comprese le attività di formazione;
- il quadro normativo sopra richiamato impone alle amministrazioni pubbliche, e in particolare ai soggetti rientranti nell'ambito di applicazione della disciplina NIS 2, l'adozione di misure organizzative, procedurali e formative idonee a garantire la gestione strutturata degli eventi e incidenti di sicurezza informatica, la definizione dei flussi di escalation e notifica, la tracciabilità delle attività svolte e il rafforzamento continuo delle competenze del personale.

Rilevato che:

- la D.G.R. n. 663/2023 ha affidato al Responsabile per la Transizione al Digitale, in coerenza con la complessiva strategia regionale sull'ICT, il coordinamento, la governance e la definizione degli indirizzi strategici del Data Center regionale e del CSIRT della Regione Puglia;
- la D.G.R. n. 1793/2024 ha disposto che il Computer Security Incident Response Team (CSIRT) Puglia sia convertito in CSIRT della Regione Puglia, confermando che l'erogazione dei servizi resta affidata a InnovaPuglia S.p.A., mentre coordinamento e governance restano nella competenza della Regione Puglia, per il tramite del RTD;
- con Determinazione Dirigenziale n. 8 del 30 dicembre 2024 sono stati approvati i documenti organizzativi del CSIRT della Regione Puglia;
- con nota del 6 maggio 2025, acquisita al prot. regionale n. 236135/2025, l'Agenzia per la cybersecurity Nazionale ha attestato il raggiungimento del livello di maturità base del modello di governo del CSIRT della Regione Puglia secondo il framework SIM3 di ENISA;
- il complesso documentale predisposto costituisce attuazione del modello strategico regionale della cybersecurity e si pone quale strumento unitario per il rafforzamento delle capacità organizzative, procedurali e formative della Regione Puglia.

Rilevato altresì che:

- il Responsabile per la Transizione al Digitale della Regione Puglia, nel biennio 2024-2025, ha pianificato le attività propedeutiche alla gestione degli eventi e degli incidenti in materia di cybersecurity previsti dal Piano di Potenziamento della cybersecurity della Regione Puglia con il supporto operativo di InnovaPuglia S.p.A., a supporto degli Enti del sistema regionale, delle strutture interne e dei soggetti coinvolti nell'attuazione della normativa NIS 2 e della Legge n. 90/2024;
- la procedura di gestione degli eventi e degli incidenti di sicurezza e il Registro degli incidenti, costituiscono, pertanto, strumenti organizzativi essenziali per assicurare la programmazione, l'attuazione e la tracciabilità delle attività richieste dal quadro normativo vigente e per garantire la formale approvazione dei relativi documenti da parte degli organi direttivi.

Rilevato infine che:

- la presente deliberazione non introduce modifiche all'assetto organizzativo regionale vigente in materia di cybersecurity, ma si pone in continuità con il modello strategico regionale già approvato, del quale costituisce attuazione sotto il profilo organizzativo, procedurale e formativo;

- i documenti allegati al presente provvedimento rappresentano strumenti attuativi essenziali per la formalizzazione del sistema regionale per la programmazione, attuazione e tracciabilità delle attività formative in materia di cybersecurity;
- l'approvazione dei predetti documenti da parte della Giunta regionale consente di consolidare un quadro unitario, coerente e formalizzato di riferimento per l'Amministrazione regionale, in conformità al modello strategico regionale della cybersecurity e agli obblighi previsti dalla disciplina nazionale ed europea di settore;
- risulta, pertanto, necessario approvare, quali parti integranti e sostanziali del presente provvedimento, i seguenti documenti:

    - Allegato A - Procedura di gestione degli eventi e degli incidenti di sicurezza informatica relativi alla Regione Puglia;
    - Allegato B - Registro incidenti della Regione Puglia

Alla luce delle risultanze istruttorie si ritiene necessario

sottoporre alla Giunta regionale, ai sensi dell'art. 4, comma 4, della L.R. n. 7/1997, l'approvazione dei documenti attuativi regionali in materia di gestione degli eventi e degli incidenti di sicurezza informatica, allegati al presente provvedimento quali parti integranti e sostanziali, al fine di assicurare la piena attuazione del modello strategico regionale della cybersecurity e la conformità dell'Amministrazione regionale al quadro normativo nazionale ed europeo di settore.

Garanzie di riservatezza

La pubblicazione sul BURP, nonché la pubblicazione sull'Albo o sul sito Istituzionale, salve le garanzie previste dalla legge 241/1990 in tema di accesso ai documenti amministrativi, avviene nel rispetto della tutela della riservatezza dei cittadini secondo quanto disposto dal Regolamento UE n. 679/2016 in materia di protezione dei dati personali, nonché dal D. Lgs. 196/2003 ss.mm.ii. ed ai sensi del vigente Regolamento regionale 5/2006 per Il trattamento dei dati sensibili e giudiziari in quanto applicabile. Ai fini della pubblicità legale, il presente provvedimento è stato redatto in modo da evitare la diffusione di dati personali identificativi non necessari ovvero il riferimento alle particolari categorie di dati previste dagli articoli 9 e 10 del succitato Regolamento UE.

Esiti Valutazione di impatto di genere: Neutro

SEZIONE COPERTURA FINANZIARIA DI CUI AL D. LGS. 118/2011 E SS. MM. E II.

La presente deliberazione non comporta implicazioni, dirette e/o indirette, di natura economico-finanziaria e/o patrimoniale e dalla stessa non deriva alcun onere a carico del bilancio regionale.

Tutto ciò premesso, al fine di procedere all'approvazione dei documenti attuativi regionali previsti dal Piano di Potenziamento della Cybersecurity della Regione Puglia, in materia di gestione degli eventi e degli incidenti di sicurezza informatica, ai sensi dell'art. 4, comma 4, della L.R. n. 7/1997, si propone alla Giunta regionale:

1. di approvare i documenti attuativi regionali in materia di gestione degli eventi e degli incidenti di sicurezza informatica, allegati alla presente deliberazione quali parti integranti e sostanziali, come di seguito indicati:

   - Allegato A - Procedura di gestione degli eventi e degli incidenti di sicurezza informatica relativi alla Regione Puglia;
   - Allegato B - Registro incidenti della Regione Puglia.

2. di dare atto che i documenti di cui al precedente punto costituiscono il quadro attuativo regionale in materia di gestione degli eventi e degli incidenti di sicurezza informatica, in coerenza con il modello strategico regionale della cybersecurity e con la disciplina nazionale ed europea di settore;

3. di demandare al Dipartimento per la Transizione Digitale il coordinamento dell'attuazione dei documenti approvati con il presente provvedimento, nell'ambito delle funzioni di governance regionale della cybersecurity, ferme restando, nei singoli documenti allegati, le attribuzioni del Referente per la cybersecurity per i profili di competenza;

4. di demandare alla Sezione Cloud, Cybersecurity e Infrastrutture Tecnologiche l'adozione dei conseguenti atti organizzativi e gestionali di competenza, nonché l'attuazione delle misure necessarie a dare esecuzione ai documenti approvati con il presente provvedimento;
5. di stabilire che eventuali modifiche ed integrazioni non sostanziali dei documenti approvati con il presente provvedimento, che si rendano necessarie e/o opportune ai fini dell'aggiornamento operativo, organizzativo o normativo, siano adottate con atto della Dirigente della Sezione Cloud, Cybersecurity e Infrastrutture Tecnologiche, nel rispetto degli indirizzi del Dipartimento per la Transizione Digitale e ferme restando, nei singoli documenti allegati, le attribuzioni del Referente per la cybersecurity per i profili di competenza;

6. di dare atto che restano ferme, per eventuali modifiche sostanziali dei documenti approvati con il presente provvedimento, le competenze degli organi regionali secondo il vigente assetto organizzativo e ordinamentale;

7. di notificare il presente provvedimento, a cura del Dipartimento per la Transizione Digitale, ai soggetti interessati;

8. di demandare al Dipartimento per la Transizione Digitale e alla Sezione Cloud, Cybersecurity e Infrastrutture Tecnologiche gli adempimenti amministrativi di rispettiva competenza per l'esatta esecuzione del presente provvedimento;
9. *di disporre la pubblicazione del presente provvedimento ad eccezione degli allegati A e B nel Bollettino Ufficiale della Regione Puglia;*

10. *di dare atto che il presente provvedimento è soggetto a pubblicazione ai sensi dell'art. 23 del D. Lgs 14 marzo 2013, n. 33, ad eccezione degli allegati A e B, sul sito istituzionale della Regione Puglia, nella sezione "Amministrazione Trasparente", sottosezione "Provvedimenti".*

I sottoscritti attestano la regolarità amministrativa dell'attività istruttoria e della proposta, ai sensi dell'art. 5, co.3, lett. da a) ad e) delle Linee guida sul "*Sistema dei controlli interni nella Regione Puglia*", adottate con D.G.R. n. 1397 del 07 ottobre 2025.

L'Istruttore
(Dott. Francesco Paolo de Meo)
FRANCESCO PAOLO
DE MEO
29.07.2026 13:34:17
GMT+02:00

Il Funzionario E.Q.
"Strategie di Cybersecurity e compliance
normativa del Progetto Clinical SOC"
(Dott. Nicola Lombardi)

Nicola Lombardi
29.07.2026 14:22:38
GMT+02:00

La Dirigente della Sezione Cloud,
Cybersecurity e Infrastrutture tecnologiche
(Dott.ssa Angela Guerra)

ANGELA
GUERRA
29.07.2026
15:07:02
GMT+02:00

Il Direttore del Dipartimento ai sensi degli artt. 18 e 20 del Decreto del Presidente della Giunta regionale 22 gennaio 2021, n. 22 e ss.mm.ii., NON RAVVISA la necessità di esprimere osservazioni alla presente proposta di D.G.R.

Il Direttore del Dipartimento per la Transizione Digitale
(Ing. Cosimo Elefante)

REGIONE PUGLIA
COSIMO ELEFANTE
30.07.2026 11:01:43
GMT+02:00

L'Assessore al Bilancio e Personale, ai sensi del vigente Regolamento della Giunta Regionale,

PROPONE

alla Giunta Regionale l'adozione del presente atto.

L'Assessore al Bilancio e Personale
(Sebastiano Giuseppe Leo)

Leo
Sebastiano Giuseppe
30.07.2026
11:06:25
UTC