# Messaggio

| numero | data | competenza |
|---|---|---|
| **8556** | 26 marzo 2025 | DIPARTIMENTO DELLE FINANZE E DELL'ECONOMIA |

## Aggiornamento delle infrastrutture tecniche e implementazione della seconda sala server ridondante per il Centro dei sistemi informativi: richiesta di un credito complessivo di 16'219'324 franchi e di un credito annuale a gestione corrente di complessivi 7'270'025 franchi per il periodo 2026-2028

Signor Presidente,
signore deputate e signori deputati,

con il presente messaggio sottoponiamo la richiesta per lo stanziamento di un credito di investimento a favore dell'aggiornamento delle infrastrutture tecniche del Centro dei sistemi informativi (CSI) per un totale di fr. 16'219'324.-, così ripartiti:

- progettazione, coordinamento e collegamento nuova sala server: fr. 2'140'380.-;
- aggiornamento infrastruttura server e banche dati: fr. 12'889'844.-;
- nuova soluzione di orchestrazione per il ripristino in caso di disastro (disaster recovery): fr. 1'189'100.-.

### I. INTRODUZIONE

Il Centro sistemi informativi ha per missione la progettazione e la fornitura delle infrastrutture di rete e di telecomunicazione, delle componenti hardware centrali, locali e periferiche, nonché delle applicazioni centrali, dipartimentali, di gruppo e individuali per garantire lo svolgimento dei compiti dell'Amministrazione cantonale (AC), definiti dal Consiglio di Stato.

Oltre alle operazioni necessarie alla progettazione ed alla fornitura delle infrastrutture, dei sistemi e delle applicazioni, il CSI fornisce la necessaria consulenza e l'indispensabile supporto per garantirne la qualità e la relativa operativà alle unità amministrative.

Il CSI è il punto di riferimento per tradurre concretamente le iniziative dell'Amministrazione Cantonale in ambito di informatizzazione, digitalizzazione e intelligenza artificiale.

Nei sistemi gestiti presso il CSI sono raccolti, gestiti e assicurati i dati dell'intera AC: dalla posta elettronica ai dati degli applicativi dipartimentali. Queste informazioni sono il cuore pulsante dell'organizzazione e permettono il corretto funzionamento dell'Amministrazione.

Da diversi anni la domanda di nuove soluzioni IT è in rapida ascesa, così come lo è l'esigenza di incrementare la sicurezza; considerata la strategia per la trasformazione digitale in corso, queste tendenze saranno ancora più marcate.

Parallelamente al messaggio di strategia per la trasformazione digitale, il CSI ha quindi approfondito le necessità tecniche e infrastrutturali dell'Amministrazione cantonale

necessarie a sostenere l'attuale e futura crescita di servizi IT legati al processo di trasformazione digitale e mitigare al contempo i rischi ambientali e cibernetici che evolvono di pari passo con l'evoluzione tecnologica. In questo senso, entrambi i messaggi sostengono in modo verticale il principio della digitalizzazione nell'Amministrazione: uno per quanto attiene i servizi "business" (strategia concernente la trasformazione digitale) e l'altro per gli aspetti architetturali e di sicurezza che sostengono la strategia digitale complessiva (aggiornamento dell'infrastruttra tecnica del CSI).

L'oggetto del presente messaggio mira inoltre a mitigare i principali rischi a cui, oggi giorno, un fornitore di servizi IT e di riflesso l'AC è confrontato:

- interruzioni fisiche o naturali come eventi naturali, guasti elettrici, allagamenti o incendi;
- attacchi informatici e software malevoli atti a sottrarre informazioni oppure a compromettere l'operatività anche, ma non solo, a fini del pagamento di un riscatto;
- perdita o corruzione accidentale di dati per eventi imprevisti;
- crescita improvvisa e non pianificata della domanda di infrastrutture tecniche;
- mancanza o riduzione delle risorse specializzate, sia per la gestione ordinaria così come per i sistemi IT tecnologicamente non più attuali.

Considerando la pervasività delle soluzioni IT in ogni unità amministrativa, l'impatto dei rischi sopra esposti si tradurrebbe in blocchi più o meno estesi dell'operatività e di riflesso sulla capacità dello Stato di assolvere i compiti assegnati per legge.

Al fine quindi di poter proseguire a ottemperare al suo mandato, è necessario che il CSI possa rinnovare le proprie infrastrutture e dotarsi delle necessarie tecnologie per rispondere in modo adeguato alle sfide odierne e future a cui è chiamato mitigando in modo adeguato i rischi.

## II. SITUAZIONE ATTUALE

### Ubicazione infrastrutture tecniche

Il CSI è ubicato in uno stabile degli anni '90 a Bellinzona, stabile che nel corso degli anni è stato l'unico punto in cui tutte le infrastrutture tecniche, centrali per l'operatività dell'AC, hanno trovato collocazione.

Le sale tecniche sono infatti tutte poste in questo stabile e assicurano oggigiorno la pressochè totalità degli applicativi impiegati dalle unità amministrative (UA) dello Stato. In numeri concreti si possono annoverare più di 50 server fisici e 700 virtuali necessari al buon funzionamento di altrettanti servizi applicativi.

In questa locazione sono presenti anche i servizi di telecomunicazione, di salvataggio dati e di gestione della sicurezza informatica.

Lo stabile ospita anche la gran parte dei collaboratori del CSI, situazione già oggetto di alcune proposte d'intervento da parte della Sezione della logistica (SL) che vedrà un messaggio separato per la sua attualizzazione.

### Infrastruttura server e banche dati

La sala server locata a Bellinzona alloggia oggi tutte le infrastrutture tecniche impiegate dal CSI.

L'attuale architettura si basa principalmente sull'impiego di tecnologie adottate nel corso degli anni ed aggiornate in modo progressivo ogni qualvolta vi erano esigenze specifiche. Quanto impiegato è infatti frutto di progetti degli ultimi 25 anni, progetti che hanno privilegiato una visione verticale piuttosto che orizzontale.

Questo approccio mostra oggi però dei limiti sia sotto un profilo di gestibilità dell'infrastruttura nel suo complesso, sia a livello di prestazioni. È quindi importante aggiornare le infrastrutture tecniche applicando un approccio moderno e allineato allo stato dell'arte del settore IT.

### Sicurezza IT

Gli strumenti per la sicurezza informatica impiegati oggi prevedono, in larga maggioranza, l'impiego di tecnologie per le difese perimetrali. L'obiettivo principale è mitigare eventuali accessi indebiti alla rete cantonale, traguardo raggiunto abbinando una stretta politica di misure di sicurezza anche sulle postazioni di lavoro locali.

Accanto alle misure tecniche viene continuamente promossa una campagna attiva di formazione dei collaboratori dell'AC con l'intento di fornire le competenze necessarie a gestire consapevolmente le nuove tecnologie.

L'evoluzione delle minacce è però sempre più accelerata e richiede ogni giorno maggiori risorse per poterla gestire e mitigare attivamente. Gli strumenti necessari per fronteggiare le minacce sono parimenti in continua evoluzione ed è importante, ai fini di mantenere un alto grado di protezione dell'infrastruttura e dei dati, che tali strumenti siano continuamente potenziati e mantenuti.

### Gestione dei ripristini in caso di disastro

Alcuni eventi imprevisti del recente passato hanno richiesto l'attivazione di un ripristino dell'operatività in caso di disastro, in inglese denominato "disaster recovery".

In particolare, l'evento del 2017[1] ha messo in evidenza la necessità di disporre di piani di ripristino efficaci e per quanto possibile automatizzati. Affidarsi a procedure esclusivamente manuali per fronteggiare situazioni di crisi di grande portata non è più percorribile. In quell'occasione l'evento impattò l'insieme di tutti i servizi dell'AC dipendenti dall'infrastruttura di Bellinzona richiedendo un intervento urgente e prolungato su 3 giorni interi di lavoro, notti comprese. I costi dervianti dalle sole attività di ripristino della parte tecnica si sono attestati a poco meno di fr. 180'000.-. Ciò nonostante gli oneri più importanti derivanti dal fermo dei servizi dell'AC, come ad esempio la chiusura degli sportelli della Sezione della circolazione, l'interruzione dell'operatività della centrale di Polizia e della giustizia, sono di difficile quantificazione. A complemento di quanto esposto, va considerato anche l'importante danno d'immagine.

La crescita dei servizi IT avvenuta in questi ultimi anni in termini numerici, di complessità e di interrelazione tra di essi, aumenta di conseguenza l'esigenza di poter far fronte in modo efficace ad eventuali interruzioni che dovessero verificarsi, situazione che andrà ad accentuarsi con il processo di trasformazione digitale. Un fermo prolungato causerebbe enormi disservizi e impatti innumerevoli sull'utenza e i servizi al cittadino.

[1] Evento che ha visto l'interruzione improvvisa e non pianificata dell'erogazione dell'energia elettrica per l'intero stabile del CSI a Bellinzona con conseguente interruzione non gestita dei servizi IT.

Le attuali procedure, perlopiù manuali, richiedono un coordinamento umano tra i differenti centri di competenza tecnici del CSI e delle UA. Questo approccio permette di principio di ripristinare le infrastrutture tecniche, ma esige al contempo un importante onere di gestione e coordinamento. Inoltre, le procedure attualmente disponibili, non permettono di mitigare alcuni rischi soprattutto in ambito di software malevoli, aspetto che graverebbe ulteriormente sulle tempistiche.

È quindi essenziale nel contesto dell'attuale crescita, e a fronte delle sempre nuove e sofisticate minacce, essere in grado di coordinare ed organizzare al meglio tutto quanto necessario ad affrontare una situazione di disastro. Esistono oggi sul mercato soluzioni e strumenti efficaci che permettono di gestire situazioni di crisi e che consentono di azzerare o limitare in modo importante i disservizi e i fermi.

## III. PROPOSTE DI INTERVENTO

Grazie ad un progetto della Sezione del militare e della protezione della popolazione si è presentata l'opportunità di disporre di una seconda sala server ubicata presso la nuova struttura al Monte ceneri. Questo progetto ha quindi dato avvio ad una prima fase, esplorativa, con la quale valutare nuovamente l'architettura tecnica nel suo complesso e come poter sfruttare al meglio sia la seconda sala macchine sia le nuove tecnologie.

A questo fine sono state organizzate diverse sessioni di lavoro sia interne al CSI che con altri Cantoni, oltre che con realtà del territorio, con l'obiettivo di valutare con un approccio olistico e innovativo il futuro impiego.

A tal proposito sono state acquisite diverse informazioni, in modalità esplorativa e non vincolante, al fine di allestire un budget da presentare in questo messaggio. Tali informazioni saranno successivamente approfondite in fase di progettazione e attraverso l'allestimento di appalti pubblici.

Di seguito vengono riassunti i principali assi d'intervento e la relativa ipotesi di spesa.

### Nuova ubicazione aggiuntiva per le infrastrutture tecniche

Grazie al progetto per l'ampliamento del posto comando per il Consiglio di Stato e l'edificazione di una nuova struttura protetta per la protezione della popolazione (SMPP) a Rivera, si è potuto ricavere una nuova sala server da poter dedicare alle infrastrutture tecniche del CSI.

Notoriamente nelle soluzioni IT disporre di più ubicazioni tecniche, a debita distanza, permette di mitigare alcuni rischi sostanzialmente legati alle questioni ambientali e fisiche come incendi, allagamenti o altri eventi maggiori. Permette inoltre di migliorare i tempi di ripristino in caso di eventi di una certa rilevanza e garantire parimenti l'attuazione di buone pratiche del mondo IT, quali ad esempio il salvataggio dati in più località.

Diversi Cantoni si appoggiano a soluzioni su più sale dislocate, tra questi troviamo ad esempio Jura, Vallese, Basilea, Svitto, Neuchatel e Ginevra. La città di Lugano, così come ad esempio la città di Losanna, hanno adottato questo approccio. Non da ultimo anche USI e SUPSI hanno in funzione due datacenter, uno a Lugano-Viganello e il secondo a Mendrisio.

I costi edili per lo stabile e le infrastrutture di base, quali ad esempio il sistema di alimentazione, di raffreddamento e l'impianto contro gli incendi, sono già stati computati dalla SMPP.

La nuova sala server andrà però progettata debitamente sia a livello architetturale che a livello di interconnessione: questi costi, come quelli dei prossimi ambiti d'intervento, saranno presentati al capitolo "conseguenze di natura finanziaria".

**Aggiornamento infrastruttura server e banche dati**

Le analisi effettuate hanno evidenziato la necessità di adottare nuove tecnologie che, di principio, offrono buoni margini di miglioramento nell'ambito gestionale. Al contempo queste nuove tecnologie garantiscono un grado di estensibilità futura decisamente più favorevole rispetto alla situazione attuale, permettendo quindi di capitalizzare l'investimento su tempistiche più lunghe.

Le valutazioni sono quindi state effettuate considerando i principi contenuti nella strategia di trasformazione digitale del Canton Ticino, e nello specifico disporre di servizi resilienti, accessibili 24 ore al giorno 7 giorni su 7 e che garantiscano la continuità operativa anche in situazioni critiche. Inoltre la crescita attuale, già di per se importante, sarà sicuramente rafforzata all'adozione della strategia e richiederà ulteriori risorse tecniche a sostegno dei nuovi strumenti. Questo aspetto, di per sé già riscontrato oggi, potrà essere meglio assorbito dalla modularità delle nuove tecnologie, caratteristica di cui gli esempi esplorati sul territorio mostrano indubbi vantaggi rispetto alla situazione attuale.

La progettazione di dettaglio sarà frutto di una fase specifica che sarà finanziata con il credito oggetto del presente messaggio. Si possono tuttavia già considerare alcuni interventi essenziali. Tra questi troviamo la trasformazione di servizi, come ad esempio la rete, la sicurezza o le banche dati, verso un concetto di ridondanza e resilienza operato in entrambe le sale server in modo parallelo. Questo aspetto è fondamentale per poter garantire a pieno lo sfruttamento del concetto di ridondanza geografica e, al contempo, migliorare sensibilmente la resilienza in caso di problemi su una singola sala server. Servizi ridondati inoltre permettono una gestione senza interruzione: sarà infatti possibile intervenire singolarmente in una delle due sale senza che queste attività si traducano in disservizi o blocchi per cittadini e funzionari. L'approccio di poter garantire la continuità e, di principio, eliminare eventuali interruzioni è essenziale per lo sviluppo di servizi IT resilienti e orientati al cittadino, così come proposto nella strategia di trasformazione digitale.

**Nuova soluzione per la sicurezza IT**

Con l'avvento di nuove minacce per la sicurezza, sempre più sofisticate, automatizzate ed efficaci, si rende necessario munirsi di strumenti di egual misura capaci di identificare, comprendere e mitigare in tempo reale eventi indebiti all'interno dell'infrastruttura.

La dislocazione geografica di due sale server amplifica la necessità di una dotazione di strumenti di questa tipologia al fine di garantire una gestione adeguata della cyber sicurezza.

Per questo motivo è necessario l'acquisizione di un Security Information Event Management (SIEM) e di un Security Orchestrator, Automation and Response (SOAR).

Tali strumenti, mediante il monitoraggio costante dei vari dispositivi critici, permettono l'identificazione precoce di situazioni potenzialmente dannose, il blocco delle attività ed il trattamento immediato attraverso contromisure automatizzate.

**Nuova soluzione per la gestione dei ripristini in caso di disastro**

Il concetto di gestione dei ripristini in caso di disastro, in inglese "disaster recovery", mira generalmente a riportare a livello operativo un determinato ambito dopo un evento dannoso imprevisto.

A questo fine sono stati concepiti degli strumenti tecnici per aiutare le imprese a riprendersi rapidamente grazie all'automazione delle attività, quali ad esempio i ripristini di emergenza automatici e coordinati, configurabili in base alle priorità operative dello Stato.

Queste soluzioni permettono in sostanza di concepire, implementare, documentare e testare le attività in situazioni di emergenza a garanzia di futuri eventi.

È da notare che, per quanto concerne il mandato svolto dal CSI, tale attività si concentra sui sistemi IT e i relativi servizi. L'ambito considerato non contempla le attività legate agli stabili ove sono operative le unità amministrative dell'AC né tantomeno le questioni funzionali necessarie nei singoli Uffici.

**Pianificazione di massima**

L'intervento previsto, secondo una prima pianificazione di massima da affinare ed aggiornare durante la fase di progettazione esecutiva, prevede una tempistica di 4 anni.

Di seguito sono riassunte le principali fasi.

| | **2025** | | **2026** | | **2027** | | **2028** | |
|---|---|---|---|---|---|---|---|---|
| | S1 | S2 | S1 | S2 | S1 | S2 | S1 | S2 |
| **Iter legislativo presso il GC** | X | | | | | | | |
| **Concorso per la progettazione esecutiva** | | X | | | | | | |
| **Progettazione esecutiva** | | X | X | | | | | |
| **Concorso infrastrutture tecniche** | | | X | X | | | | |
| **Fornitura, installazione e configurazione** | | | | X | X | X | X | X |
| **Collaudo e termine progetto** | | | | | | | | X |

## IV. CONSEGUENZE DI NATURA FINANZIARIA

Per definire le conseguenze di natura finanziaria, il CSI ha svolto un'analisi esplorativa e non vincolante, al fine di allestire un budget da presentare in questo messaggio. Questa attività ha potuto contare su elementi concreti assunti da fornitori conosciuti, così come da indicazioni basate su scenari analoghi in altre realtà. Tali informazioni dovranno essere approfondite in fase di progettazione. Evidentemente le singole prestazioni saranno definite e deliberate conformemente alle disposizioni previste nell'ambito della legislazione sulle commese pubbliche, attraverso l'allestimento di appalti pubblici.

| **Ambito** | **Investimento (fr.)** | **Gest. corrente, dal 2028 (fr.)** |
|---|---|---|
| **1 Nuova ubicazione**<br>Progettazione e coordinamento attività<br>Interconnessione di rete | **1'800'000** | **280'000** |
| **2 Aggiornamento infrastruttura server e banche dati**<br>Aggiornamento banche dati<br>Ampliamento servizi di backup<br>Soluzione Infrastructure as a Service (IaaS) per Mainframe<br>Sistemi di storage (infrastruttura per la salvaguardia dei dati)<br>Sistemi di iperconvergenza (nuovo concetto di virtualizzazione server) | **10'840'000** | **1'500'000** |
| **3 Nuova soluzione per la sicurezza IT**<br>SIEM e SOAR | **-** | **720'000** |
| **4 Licenze applicative** | **1'000'000** | **250'000** |
| **IVA 8.1%** | **1'104'840** | **222'750** |
| **Riserva 10%** | **1'474'484** | **297'275** |
| **TOTALE** | **16'219'324** | **3'270'025** |

In sintesi, queste proposte determinano le seguenti conseguenze di natura finanziaria:

- spese di investimento: fr. 16'219'324.-
- spese di gestione corrente annue a regime: fr. 3'270'025.-

Nei costi relativi alla gestione corrente sono considerate le licenze, i servizi IT e quanto necessario alla interconnessione di rete tra le due infrastrutture.
L'impatto sulla gestione corrente sarà graduale nel tempo: fr. 1'500'000.- per l'anno 2026, fr. 2'500'000.- per il 2027 e, a partire dal 2028, fr. 3'270'025.-.

Non è previsto un impatto sull'effettivo del personale.

Lo stanziamento dei crediti proposti con l'allegato decreto legislativo richiedono l'approvazione da parte della maggioranza assoluta dei membri del Gran Consiglio (cfr. art. 5 cpv. 3 LGF).

## V. RELAZIONE CON LE LINEE DIRETTIVE E IL PIANO FINANZIARIO

Le seguenti proposte sono integrate nel piano finanziario 2024-2027.

### Collegamenti con il piano finanziario degli investimenti

Il credito è inserito nel piano finanziario degli investimenti 2024-2027, nell'ambito del settore 11, amministrazione generale, posizione 114 980 9.

Il credito per gli interventi è previsto al WBS 951 50 3029 "Aggiornamento infrastruttura IT" (conto 50600017 "Progetti informatici") per un importo di fr. 16'219'324.-.

### Collegamenti con il piano finanziario di gestione corrente

Gli interventi di adeguamento previsti comportano variazioni di fr. 3'270'025.- (a regime, dal 2028) sugli attuali costi di esercizio. Di conseguenza, il preventivo a gestione corrente del CSI dovrà essere modificato come segue:

- fr. 237'820.- per la manutenzione delle apparecchiature di telecomunicazione (CRB 952, conto 31530008 "Manutenzione apparecchiature telecomunicazioni");
- fr. 95'128.- per le linee di comunicazione (CRB 952, conto 31300139 "Spese linee trasmissione dati e servizi telematici");
- fr. 594'550.- per la soluzione IaaS per il Mainframe (CRB 951, conto 31530005 "Manutenzione macchine, apparecchiature e PC");
- fr. 1'189'100.- per le licenze dei sistemi centrali (CRB 951, conto 31580003 "Licenze e manutenzione per elaboratore centrale e PC");
- fr. 856'152.- per le soluzioni di sicurezza, licenze e applicativi (CRB 951, conto 31580005 "Licenze e manutenzione per programmi applicativi");
- fr. 297'275.- per il sistema di ripristino d'emergenza, licenze e applicativi (CRB 951, conto 31580005 "Licenze e manutenzione per programmi applicativi").

### Conseguenze sul personale

Queste proposte non avranno ripercussioni sugli effettivi del personale.

## VI. CONSEGUENZE A LIVELLO DI ENTI LOCALI

Non sono previste conseguenze a livello di Enti locali.

## VII. CONSEGUENZE AMBIENTALI

Le proposte contenute nel presente messaggio apporteranno delle conseguenze ambientali positive nella misura in cui le nuove tecnologie permetteranno un minor consumo di energia e, parimenti, permetteranno di estendere e non sostituire quanto realizzato a fronte di una crescente domanda di nuovi strumenti IT. Indirettamente, ogni nuova soluzione IT contribuirà a ridurre lo spreco di carta e di tempo per trattare le informazioni.

## VIII. CONCLUSIONI

La tecnologia dell'informazione è uno strumento di lavoro fondamentale per una parte sempre più consistente dell'Amministrazione cantonale. Senza questo supporto sono preclusi l'accesso ad informazioni, processi e, in ultima analsisi, l'operatività dei servizi dello Stato e il processo di trasformazione digitale.

La richiesta di nuovi strumenti IT è in costante crescita nel corso degli ultimi anni e la tendenza proseguirà anche nei prossimi anni, coerentemente con la strategia per la trasformazione digitale dello Stato. Per sostenere questo sviluppo occorre quindi adeguare anche l'infrastruttura. I due messaggi, strategia per la trasformazione digitale da un lato e aggiornamento infrastrutturale dall'altro, sono quindi complementari in quanto l'infrastruttura dovrà poter supportare le richieste derivanti dal processo di digitalizzazione.

L'ecosistema digitale porta con sé rischi che necessitano una risposta adeguata che, a fronte sia delle crescenti minacce oltre che alla crescita di soluzioni e utilizzatori, impone l'adozione di nuovi strumenti legati alla sicurezza cyber. Questi strumenti potranno rispondere repentinamente a nuove minacce e fornire risposte puntuali.

A favore di un sostanziale miglioramento sotto il profilo della resilienza, l'allestimento di una seconda sala server ridondante, collocata in un progetto edile già in costruzione da parte della Sezione del militare e della protezione della popolazione permetterà di concentrare ed efficentare le attuali operazioni effettuate in più stabili sul territorio.

L'investimento richiesto rientra quindi in un importante e fondamentale tassello a sostegno delle necessità IT dell'Amministrazione cantonale e del processo in corso di trasformazione digitale dell'AC. Per questo motivo il presente messaggio viene presentato in parallelo a quello concernente l'attuazione della prima fase della strategia per la trasformazione digitale del Cantone Ticino.

Vogliate gradire, signor Presidente, signore deputate e signori deputati, l'espressione della nostra massima stima.

Per il Consiglio di Stato

Il Presidente: Christian Vitta
Il Cancelliere: Arnoldo Coduri

Disegno di

**Decreto legislativo**
**concernente la richiesta di stanziamento di un credito di investimento di 16'219'314 franchi e di un credito annuale a gestione corrente di complessivi 7'270'025 franchi per il periodo 2026–2028**
del .....

IL GRAN CONSIGLIO
DELLA REPUBBLICA E CANTONE TICINO

visto il messaggio del Consiglio di Stato n. 8556 del 26 marzo 2025,

decreta:

**Art. 1**
È stanziato un credito di 16'219'314 franchi per l'aggiornamento delle infrastrutture tecniche presso il Centro dei sistemi informativi.

**Art. 2**
Il credito è iscritto al conto degli investimenti del Dipartimento delle finanze e dell'economia, Centro sistemi informativi.

**Art. 3**
[1]È stanziato un credito annuale ricorrente di:
- 1'500'000 franchi per l'anno 2026;
- 2'500'000 franchi per l'anno 2027;
- 3'270'025 franchi a partire dall'anno 2028.

[2]Il credito annuale è iscritto nei conti di gestione corrente del Dipartimento delle finanze e dell'economia, Centro sistemi informativi.

**Art. 4**
[1]Il presente decreto legislativo sottostà a referendum facoltativo.
[2]Esso entra in vigore immediatamente.