Il sistema Anci a supporto
della digitalizzazione
dei Comuni

DIPARTIMENTO
PER LA TRASFORMAZIONE
DIGITALE

anci

Finanziato
dall'Unione europea
NextGenerationEU

Legge 28 giugno 2024, n. 90
L'articolo 8: Rafforzamento della resilienza delle pubbliche amministrazioni e referente per la cybersicurezza.

Claudio Ciccotelli

Capo Divisione Perimetro di Sicurezza Nazionale Cibernetica
e discipline nazionali, Servizio Regolazione, ACN

Obiettivo Focus On

Fornire un orientamento rispetto ai contenuti dell'Art. 8 Rafforzamento della resilienza delle pubbliche amministrazioni e referente per la cybersicurezza - Legge 28 giugno 2024, n. 90.

Cosa prevede l'Articolo 8 della Legge 90/2024

Rafforzamento della resilienza delle pubbliche amministrazioni e referente per la cybersicurezza

- **Individuazione di una struttura** che provvede agli ambiti per il rafforzamento della resilienza
- **Individuazione del Referente** per la cybersicurezza

Struttura e ambiti di rafforzamento della resilienza

DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE

anci

Finanziato dall'Unione europea NextGenerationEU

Individuazione di una struttura, anche tra quelle esistenti, nell'ambito delle risorse umane, strumentali e finanziarie disponibili a legislazione vigente, che provvede ai seguenti ambiti:

a) sviluppo delle politiche e delle procedure di sicurezza delle informazioni

b) produzione e aggiornamento di sistemi di analisi preventiva di rilevamento e di un piano per la gestione del rischio informatico

c) produzione e aggiornamento di un documento che definisca i ruoli e l'organizzazione del sistema per la sicurezza delle informazioni dell'amministrazione

d) produzione e aggiornamento di un piano programmatico per la sicurezza di dati, sistemi e infrastrutture dell'amministrazione

e) pianificazione e attuazione di interventi di potenziamento delle capacità per la gestione dei rischi informatici, in coerenza con i piani di cui alle lettere b) e d)

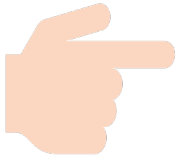
f) pianificazione e attuazione dell'adozione delle misure previste dalle linee guida per la cybersicurezza emanate dall'Agenzia per la cybersicurezza nazionale

g) monitoraggio e valutazione continua delle minacce alla sicurezza e delle vulnerabilità dei sistemi per il loro pronto aggiornamento di sicurezza

Referente per la cybersicurezza

Figura in possesso di specifiche e comprovate professionalità e competenze in materia di cybersicurezza

Opera presso la struttura individuata ai sensi dell'articolo 8



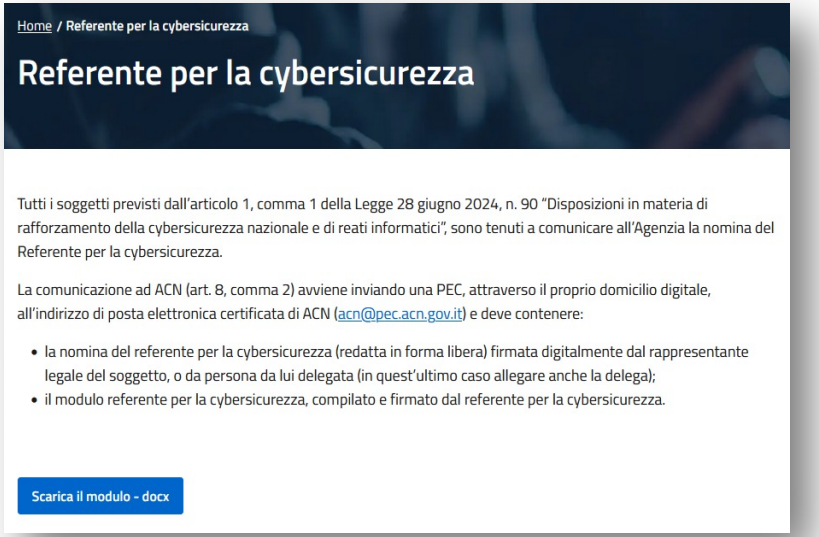
Svolge le funzioni di punto di contatto dell'amministrazione con ACN

I soggetti che non dispongono di personale dipendente in possesso di tali requisiti possono conferire l'incarico a un dipendente di una pubblica amministrazione (previa autorizzazione)

Referente per la cybersicurezza: modalità di comunicazione ad ACN

Il nominativo e gli estremi di contatto del referente sono comunicati ad ACN secondo le modalità indicate sul sito dell'Agenzia:

- **nomina firmata dal rappresentante legale** (o persona da lui delegata);
- modulo **compilato e firmato**
- trasmissione via **PEC all'ACN.**



https://www.acn.gov.it/portale/referente-per-la-cybersicurezza

Struttura e referente nelle Pubbliche Amministrazioni

La struttura e il referente possono essere individuati, rispettivamente:

- nell'**ufficio per la transizione al digitale**
- nel **Responsabile per la transizione al digitale (RTD)**

I loro **compiti** possono essere esercitati in **forma associata** (art. 17, co. 1-sexies e 1-septies del CAD)

Art. 17, co. 1-sexies e 1-septies del CAD

1-sexies. Nel rispetto della propria autonomia organizzativa, le pubbliche amministrazioni diverse dalle amministrazioni dello Stato individuano l'ufficio per il digitale di cui al comma 1 tra quelli di livello dirigenziale oppure, ove ne siano privi, individuano un responsabile per il digitale tra le proprie posizioni apicali. In assenza del vertice politico, il responsabile dell'ufficio per il digitale di cui al comma 1 risponde direttamente a quello amministrativo dell'ente.

1-septies. I soggetti di cui al comma 1-sexies possono esercitare le funzioni di cui al medesimo comma anche in forma associata.

Le disposizioni dell'articolo 8 non si applicano:

- ai soggetti inseriti nel **Perimetro di sicurezza nazionale cibernetica;**
- agli organi dello Stato preposti alla prevenzione, all'accertamento e alla repressione dei reati, alla tutela dell'ordine e della sicurezza pubblica e alla difesa e sicurezza militare dello Stato e agli organismi di informazione per la sicurezza.

Linee guida

a) sviluppo delle politiche e delle procedure di sicurezza delle informazioni

b) produzione e aggiornamento di sistemi di analisi preventiva di rilevamento e di un piano per la gestione del rischio informatico

c) produzione e aggiornamento di un documento che definisca i ruoli e l'organizzazione del sistema per la sicurezza delle informazioni dell'amministrazione

d) produzione e aggiornamento di un piano programmatico per la sicurezza di dati, sistemi e infrastrutture dell'amministrazione

e) pianificazione e attuazione di interventi di potenziamento delle capacità per la gestione dei rischi informatici, in coerenza con i piani di cui alle lettere b) e d)

f) pianificazione e attuazione dell'adozione delle misure previste dalle linee guida per la cybersicurezza emanate dall'Agenzia per la cybersicurezza nazionale

g) monitoraggio e valutazione continua delle minacce alla sicurezza e delle vulnerabilità dei sistemi per il loro pronto aggiornamento di sicurezza

Linee guida per il rafforzamento della resilienza

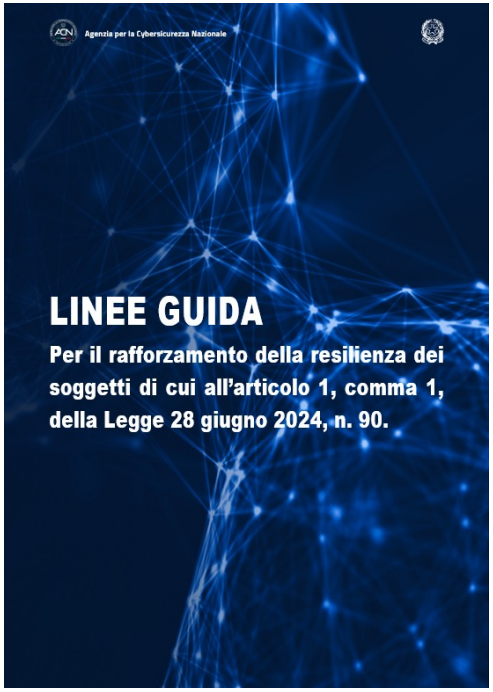
Definite in coerenza con gli ambiti di cui all'art. 8, co. 1, della Legge 90/2024 e alla Direttiva del Presidente del Consiglio dei ministri 29 dicembre 2023 (*Resilienza cibernetica del Paese - Protocolli di intesa per irrobustire la capacità di risposta agli incidenti informatici*)

PARTE 1: MISURE DI SICUREZZA

- definizione di 26 misure di sicurezza che i soggetti adottano per il rafforzamento della propria resilienza.

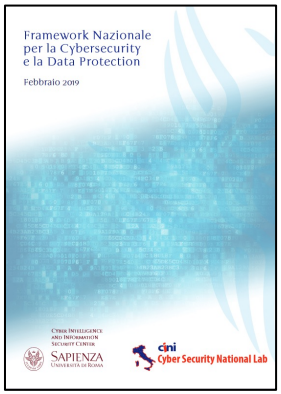
PARTE 2: MODALITÀ DI IMPLEMENTAZIONE

- supporto ai soggetti nell'implementazione delle misure di sicurezza.



Misure di sicurezza (1)

Selezione e adattamento al contesto di alcune delle subcategory del Framework Nazionale per la Cybersecurity e la Data Protection



IDENTIFY: 10 misure

- governance
- gestione asset
- gestione rischio
- supply-chain

PROTECT: 11 misure

- controllo accessi
- sicurezza dati
- gestione backup e vulnerabilità
- manutenzione sistemi
- protezione reti, piani di DR e BC
- formazione del personale

DETECT: 2 misure

- monitoraggio sistemi e reti

RESPOND: 2 misure

- piano risposta incidenti
- gestione informazioni vulnerabilità

RECOVER: 1 misura

- piano ripristino incidenti

Misure di sicurezza (2)

Per ogni misura sono indicati:

- i **requisiti** da soddisfare per l'implementazione minima attesa
- le **peculiarità** ai fini della sua implementazione
- i **contenuti dell'impianto documentale** prodotto dal soggetto
- le **modalità di implementazione** raccomandate per l'attuazione

I soggetti possono adottare modalità alternative a quelle indicate, che soddisfino le implementazioni minime attese.

Impianto documentale (1)

Impianto documentale: insieme dei documenti necessari ai fini dell'attuazione delle misure di sicurezza e dell'attestazione dell'effettiva implementazione delle stesse

- Per ciascuna misura le linee guida indicano i **contenuti minimi** che il relativo **impianto documentale** deve trattare
- In base al proprio contesto, **ciascun soggetto può decidere come organizzare il proprio impianto documentale**, ad esempio raggruppando i contenuti in un unico documento o distribuendoli tra più documenti
- L'impianto documentale può essere reso disponibile in **formato cartaceo o digitale,** purché facilmente **fruibile** da chi ha la necessità di conoscerlo e consultarlo

Impianto documentale (2)

Ogni documento dell'impianto documentale deve in ogni caso rispettare le seguenti caratteristiche:

- essere approvato dal vertice, o rappresentante legale, del soggetto o da una figura da lui formalmente delegata (come, ad esempio, quella del referente per la cybersicurezza)
- riprodurre la situazione corrente ed essere aggiornato in caso di variazioni dello stato di fatto
- essere sottoposto a revisione periodica e al verificarsi di eventi interni, eventi esterni o mutamenti dell'esposizione alle minacce e ai relativi rischi
- dare evidenza della corrispondenza dei propri contenuti con quelli richiesti dalle misure di sicurezza (evidenze documentali)

Esempio: Misura PR.IP-4 (1)

PR.IP-4

I backup delle informazioni sono eseguiti, amministrati e verificati.

Requisiti implementazione minima attesa

La seguente tabella riporta i requisiti che devono essere soddisfatti per l'implementazione minima attesa della misura.

PUNTO	REQUISITO
1	In accordo agli esiti dell'analisi del rischio di cui alla misura ID.RA-5, sono effettuati periodicamente i backup dei dati.
2	In accordo agli esiti dell'analisi del rischio di cui alla misura ID.RA-5, è assicurata la riservatezza delle informazioni contenute nei backup mediante adeguata protezione fisica dei supporti ovvero mediante cifratura.
3	In accordo agli esiti dell'analisi del rischio di cui alla misura ID.RA-5, è verificata periodicamente l'utilizzabilità dei backup effettuati mediante test di ripristino.
4	Le politiche di cybersecurity di cui alla misura ID.GV-1 includono le politiche in relazione ai punti 1, 2 e 3.
5	I processi di cybersecurity di cui alla misura ID.GV-1 includono i processi in relazione ai punti 1, 2 e 3.
6	In relazione al backup dei dati, esiste un documento aggiornato contenente almeno le procedure, metodologie e tecnologie impiegate per il rispetto delle politiche e nell'ambito dei processi di cui alla misura ID.GV-1.

Esempio: Misura PR.IP-4 (2)

Descrizione

La misura richiede – in accordo agli esiti dell'analisi del rischio di cui alla misura ID.RA-5 – di effettuare periodicamente i backup dei dati dei sistemi informativi e di rete, assicurare la riservatezza delle informazioni contenute nei backup proteggendo adeguatamente i supporti (anche tramite cifratura) e verificare periodicamente la correttezza dei backup mediante test di ripristino.

> L'analisi del rischio condotta sui sistemi informativi e di rete può infatti determinare rischi differenti a seconda della tipologia di dati trattati dai sistemi informativi e di rete. Verosimilmente saranno presenti sistemi informativi e di rete che trattano dati per i quali sono state definite politiche più stringenti in termini di RTO e RPO, di conseguenza si adotteranno strategie di backup differenti (ad esempio in termini di frequenza oppure numero di copie di backup conservate anche offline).

La misura richiede quindi di definire politiche e processi rispetto ai requisiti sopra indicati e di includerli nelle politiche e nei processi di cui alla misura ID.GV-1.

> È opportuno altresì prevedere backup dei dati relativi al monitoraggio di cui alla misura DE.CM-1.

La misura richiede infine di documentare le procedure, metodologie e tecnologie adottate per il rispetto delle politiche e nell'ambito dei processi di cui alla misura ID.GV-1 in relazione al backup dei dati.

> A tal fine, si individuano le politiche e i processi di cui alla misura ID.GV-1 relativi al *backup dei dati* (tipicamente compresi nell'ambito della *sicurezza dei dati*) e si definiscono, e documentano, le procedure, indicanti anche le metodologie e tecnologie impiegate, che implementano tali politiche e processi.

Esempio: Misura PR.IP-4 (3)

Evidenze documentali

L'impianto documentale prodotto dal soggetto deve prevedere almeno i contenuti elencati nella seguente tabella, che riporta, oltre all'indicazione dei contenuti richiesti, i requisiti dell'implementazione minima della misura ai quali i contenuti fanno riferimento.

CONTENUTO DOCUMENTO	REQUISITO
Politiche e processi relativi ai requisiti 1, 2 e 3.	1, 2, 3, 4, 5
Procedure, metodologie e tecnologie relative al backup dei dati.	1, 2, 3, 6

Esempio: Misura PR.IP-4 (4)

DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE

Finanziato dall'Unione europea NextGenerationEU

PR.IP-4

I backup delle informazioni sono eseguiti, amministrati e verificati.

Modalità di implementazione

In questo paragrafo sono riportate, sotto forma di indicazioni operative e di dettaglio, le modalità di implementazione raccomandate per l'attuazione della misura.

1. In accordo agli esiti del rischio di cui alla misura ID.RA-5, definire le politiche in relazione ai seguenti requisiti:
   a) esecuzione periodica dei backup;
   b) protezione fisica dei supporti di backup;
   c) verifica periodica dell'utilizzabilità dei backup;
2. Includere le politiche e i processi di cui al precedente punto 1 nelle politiche e nei processi di cui alla misura ID.GV-1.
3. Nel rispetto delle politiche di cybersecurity e nell'ambito del processo di sicurezza dei dati di cui alla misura ID.GV-1, definire e documentare procedure, metodologie e tecnologie impiegate, in relazione al backup dei dati.
4. Eseguire quando previsto ogni fase del processo di sicurezza dei dati relativa al backup dei dati.

DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE

Finanziato dall'Unione europea NextGenerationEU

Grazie

per la vostra attenzione

Il Sistema Anci a supporto della digitalizzazione dei Comuni