Il sistema Anci a supporto
della digitalizzazione
dei Comuni

DIPARTIMENTO
PER LA TRASFORMAZIONE
DIGITALE

anci

Finanziato
dall'Unione europea
NextGenerationEU

Introduzione alla legge sulla cybersicurezza nazionale e sui reati informatici n. 90 del 28 giugno 2024

Valentina Lo Voi

Vice Capo Divisione Consapevolezza, ACN

Obiettivo del corso

Fornire un quadro sintetico della Legge 28 giugno 2024, n. 28, in particolare:

- soggetti rilevanti
- i compiti a carico dei soggetti rilevanti
- le modifiche relative alla normativa in materia di responsabilità degli enti
- le preclusioni introdotte per il personale che abbia ricoperto ruoli particolari presso le PP.AA

Premessa: L'Agenzia per la cybersicurezza nazionale (1)

L'AGENZIA PER LA CYBERSICUREZZA NAZIONALE (ACN)

- L'architettura nazionale di cybersicurezza dopo il DL 82/2021
- L'istituzione dell'Agenzia
- Struttura dell'ACN
- Principali funzioni dell'ACN

CSIRT ITALIA
COMPUTER SECURITY INCIDENT RESPONSE TEAM

AUTORITÀ NAZIONALE COMPETENTE E PUNTO DI CONTATTO UNICO NIS

RESPONSABILE PER LA PREVENZIONE, PREPARAZIONE, GESTIONE DI CRISI CIBERNETICHE (NCS)

Premessa: L'Agenzia per la cybersicurezza nazionale (2)

La struttura dell'Agenzia

DG

VDG

Servizi

- Gabinetto
- Regolazione
- Certificazione e vigilanza
- Operazioni e gestione delle crisi cyber
- Programmi industriali tecnologici e di ricerca
- Risorse umane e amministrazione generale
- Amministrazione e bilancio
- Strategie e comunicazione

Strutture a diretto riporto del DG

Strutture a diretto riporto del VDG

DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE
anci
Finanziato dall'Unione europea NextGenerationEU

La LEGGE 28 giugno 2024, n. 90

Disposizioni in materia di rafforzamento della cybersicurezza nazionale, di **resilienza delle pubbliche amministrazioni e del settore finanziario**, di personale e funzionamento dell'Agenzia per la cybersicurezza nazionale e degli organismi di informazione per la sicurezza nonché di **contratti pubblici di beni e servizi informatici** impiegati in un contesto connesso alla tutela degli interessi nazionali strategici.

I soggetti rilevanti

DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE

Finanziato dall'Unione europea NextGenerationEU

Pubbliche amministrazioni

Soggetti PSNC

(Perimetro nazionale sicurezza cibernetica)

Soggetti NIS

(ricompresi nella direttiva NIS - network and information systems across the Union)

Soggetti TEL.CO.

(Telecomunication system)

Quali Pubbliche amministrazioni?

- Le **pubbliche amministrazioni centrali incluse nell'elenco annuale ISTAT** delle pubbliche amministrazioni
- le **regioni e le province autonome** di Trento e di Bolzano
- le **città metropolitane**
- i **comuni** con popolazione superiore a **100.000 abitanti** e i comuni **capoluoghi di regione**
- le società di **trasporto pubblico urbano** con bacino di utenza non inferiore a 100.000 abitanti
- le società di trasporto pubblico extraurbano operanti nell'ambito delle città metropolitane
- le aziende sanitarie locali
- le società in house degli enti fin qui richiamati, qualora siano fornitrici di servizi informatici, dei servizi di trasporto sopra indicati, dei servizi di raccolta, smaltimento o trattamento di acque reflue urbane, domestiche o industriali, ovvero servizi di gestione dei rifiuti.

DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE
anci
Finanziato dall'Unione europea NextGenerationEU

Gli attori pubblici

a) Dotarsi di una struttura per la cybersicurezza

b) Nominare un referente per la cybersicurezza

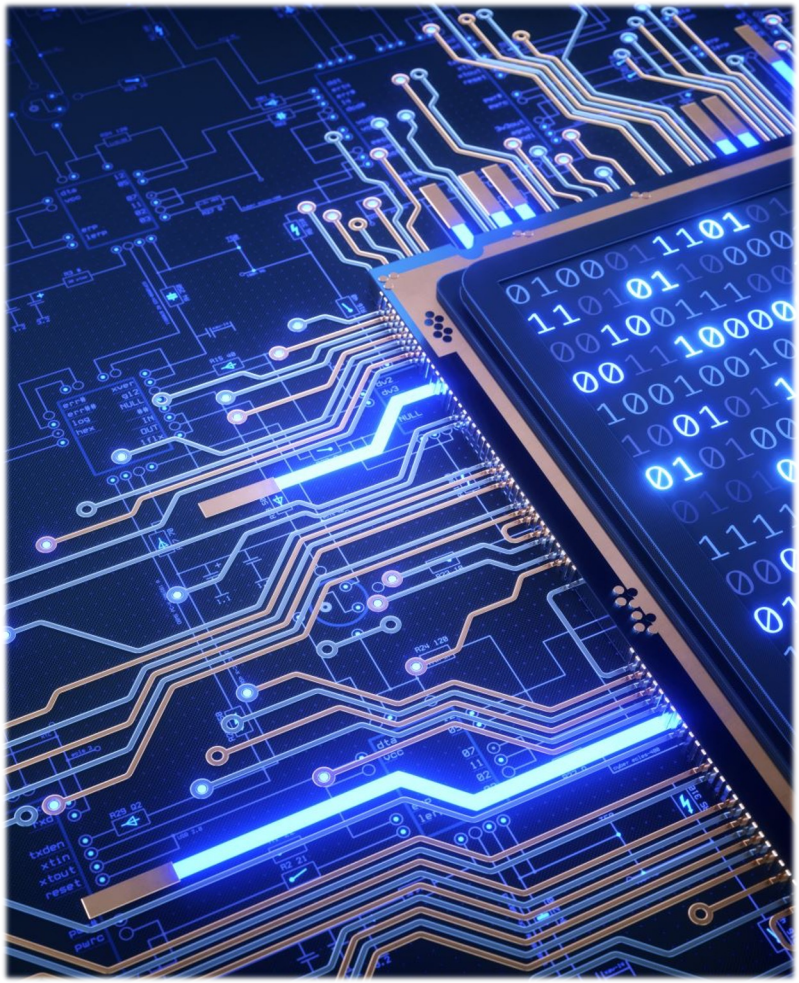
c) Comunicare gli incidenti

d) Adottare interventi risolutivi delle vulnerabilità

La struttura per la cybersicurezza: i compiti (1)

- sviluppo di **politiche e procedure** di sicurezza delle informazioni
- predisposizione e aggiornamento di un **piano per il rischio** informatico
- implementazione di sistemi di analisi preventiva di **rilevamento del rischio** informatico
- produzione e aggiornamento di un **documento che definisca i ruoli** e **l'organizzazione del sistema** per la sicurezza delle informazioni degli Attori Pubblici
- pianificazione e attuazione di **interventi di potenziamento delle capacità** per la **gestione dei rischi** informatici, a partire dai piani redatti

La struttura per la cybersicurezza: i compiti (2)



- pianificazione e attuazione dell'adozione delle **misure previste dalle linee guida** per la cybersicurezza emanate dall'Agenzia per la Cybersicurezza Nazionale (ACN)
- **monitoraggio e valutazione** continua delle minacce alla sicurezza e delle vulnerabilità dei sistemi per il loro pronto aggiornamento
- verifica che i **programmi e le applicazioni** informatiche e di comunicazione elettronica in uso presso gli Attori Pubblici che impieghino **soluzioni crittografiche** rispettino le **linee guida sulla crittografia** e quelle sulla conservazione delle password adottate dall'**ACN** e dall'**Autorità Garante per la Protezione dei Dati Personali**
- verifica che le applicazioni e i programmi menzionati non presentino **vulnerabilità** note

Il referente per la cybersicurezza

Deve essere individuato in ragione delle sue **specifiche professionalità** e **competenze** possedute in materia di cybersicurezza.

Il nominativo deve essere obbligatoriamente **comunicato all'ACN,** svolge la funzione di **punto di contatto unico** dell'**Attore Pubblico.**

Può essere individuato anche nella figura del **responsabile per la transizione al digitale**

Può essere incaricato il **dipendente** di un **altro attore** pubblico

I compiti del referente per la cybersicurezza possano essere esercitati **in forma associata**

DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE
anci
Finanziato dall'Unione europea NextGenerationEU

Diverse decorrenze

- **massimo 24 ore**, dal momento in cui l'Attore Pubblico sia venuto a conoscenza dell'incidente, per svolgere una **prima segnalazione**
- **massimo 72 ore**, dal momento in cui l'Attore Pubblico sia venuto a conoscenza dell'incidente, per svolgere la **notifica completa**, comunicando tutte le informazioni disponibili

Le sanzioni in caso di mancata ottemperanza

Cosa succede

Avviso da parte di ACN che il **reiterato inadempimento** nell'arco di 5 anni comporta l'applicazione della **sanzione amministrativa pecuniaria** da un minimo di 25.000 euro a un massimo di 125.000 euro. Possibile **responsabilità amministrativo-contabile.**

Adozione di interventi risolutivi delle vulnerabilità

Adozione di **interventi risolutivi indicati dall'ACN**, nel caso in cui siano segnalate **specifiche vulnerabilità** cui gli Attori Pubblici risultino potenzialmente esposti. I destinatari di tali segnalazioni devono **provvedere senza ritardo** – e comunque non oltre **15 giorni dalla ricezione della comunicazione –** all'adozione di tali interventi.

Le sanzioni in caso di mancata ottemperanza (segue)

Cosa succede

Avviso da parte di ACN che il **reiterato inadempimento** nell'arco di 5 anni comporta l'applicazione della **sanzione amministrativa pecuniaria** da un minimo di 25.000 euro a un massimo di 125.000 euro.

Mancata applicazione della sanzione in caso di motivate esigenze di natura **tecnico-organizzativa** che impediscano l'adozione degli interventi.

Gli adempimenti a carico degli altri soggetti rilevanti

DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE

anci

Finanziato dall'Unione europea NextGenerationEU

Soggetti PSNC
(perimetro nazionale di sicurezza cibernetica)

- Variare le tempistica dell'obbligo di notifica degli incidenti che colpiscono gli asset non inseriti nell'elenco dei beni ICT.
- Verificare che i programmi e le applicazioni informatiche rispettino le linee guida sulla crittografia e quelle sulla conservazione delle password.
- Adottare interventi risolutivi delle vulnerabilità.

Soggetti TEL.CO.
(telecomunications company)

- Adottare interventi risolutivi delle vulnerabilità.

Le modifiche alla normativa penalistica

Inasprimento della risposta sanzionatoria in relazione ad alcuni reati.

Modifiche all'art. 24 bis del D.Lgs. 231/2001

Abrogazione dell'art. 615-quinquies c.p.

Novità in materia di contratti pubblici in materia di beni e servizi informatici

Un **DPCM** da adottarsi entro **120 gg** dall'entrata in vigore della L. 90/2024 definirà dei **criteri** e delle **regole di cybersecurity** per garantire **confidenzialità, integrità** e **disponibilità dei dati.**

Vengono altresì previsti specifici **obblighi** e **facoltà** per **stazioni appaltanti** e **centrali di committenza.**

Preclusioni per il personale che abbia ricoperto ruoli specifici presso altre PP.AA

Breve riepilogo

- Introduzione sull'architettura di cybersicurezza nazionale e ACN
- La legge n. 90/2024
  - soggetti rilevanti
  - gli adempimenti in capo ai soggetti rilevanti
  - le sanzioni in caso di inottemperanza
  - le modifiche alla normativa penalistica
  - le novità in materia di contratti pubblici in materia di beni e servizi informatici
  - preclusioni per il personale che abbia ricoperto ruoli specifici presso altre PP.AA

DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE

Finanziato dall'Unione europea NextGenerationEU

Grazie

per la vostra attenzione

v.lovoi@acn.gov.it

Il Sistema Anci a supporto della digitalizzazione dei Comuni