



Transizione nazionale alla crittografia post-quantum

Ancona, 08.10.2026

Concetto di base: due categorie di crittografia



Crittografia Simmetrica

- **Una sola chiave segreta** sia per cifrare che per decifrare
- **Richiede un canale sicuro** per condividere la chiave segreta
- **Algoritmi efficienti**, adatti a processare grandi quantità di dati
- Utilizzi: **cifratura** dati in transito e a riposo
- **Attualmente resistente** alla minaccia quantistica (accorgimenti minimi)



Crittografia a Chiave Pubblica

- **Due chiavi**, una per cifrare e una per decifrare
- **Non richiede canali sicuri**
- **Schemi inefficienti** per processare grandi quantità di dati
- Utilizzi: **scambio chiave** simmetrica, **firma digitale**
- **Schemi vulnerabili** alla minaccia quantistica (algoritmo di Shor)

Harvest now, decrypt later

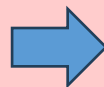
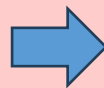
Schemi post-quantum

Sistemi implementabili sui **computer classici** che si basano su **problemi matematici resistenti** agli attacchi quantistici

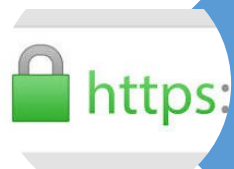
Gli algoritmi standardizzati nel 2024 sono stati sottoposti nel 2016.

(8 anni e oltre)

Nuova gara NIST partita nel 2022 per ottenere altri algoritmi alternativi di firma
(tutt'ora in corso)

Contesto	Schemi attuali	Schemi post-quantum
Scambio chiave	- RSA - DH(E) - ECDH(E) 	- ML-KEM (STD) - HQC-KEM (selezionato per STD)
Firma digitale	- RSASSA - DSA - ECDSA 	- ML-DSA (STD) - SLH-DSA (STD) - FN-DSA (selezionato per STD) - Nuovi algoritmi alternativi?

Ambito di impiego della crittografia a chiave pubblica



Comunicazioni internet
(HTTPS, TLS, IPsec)



App di pagamento
(ApplePay, GooglePay)



Carte bancarie e servizi
bancari online



SPID e identità digitale



Carta d'identità
elettronica e passaporti



Messaggistica sicura
(end-to-end encryption)



Firma digitale dei
documenti (FEQ)



Blockchain, crittovalute,
Trusted Platform (HSM
TPM....)

Minaccia



Transizione alla Post-Quantum Cryptography

Indicazioni UE



La Roadmap impone 3 **milestone** fondamentali:

Entro il 31.12.2026



Stabilire Piano Nazionale di transizione

Entro il 31.12.2030



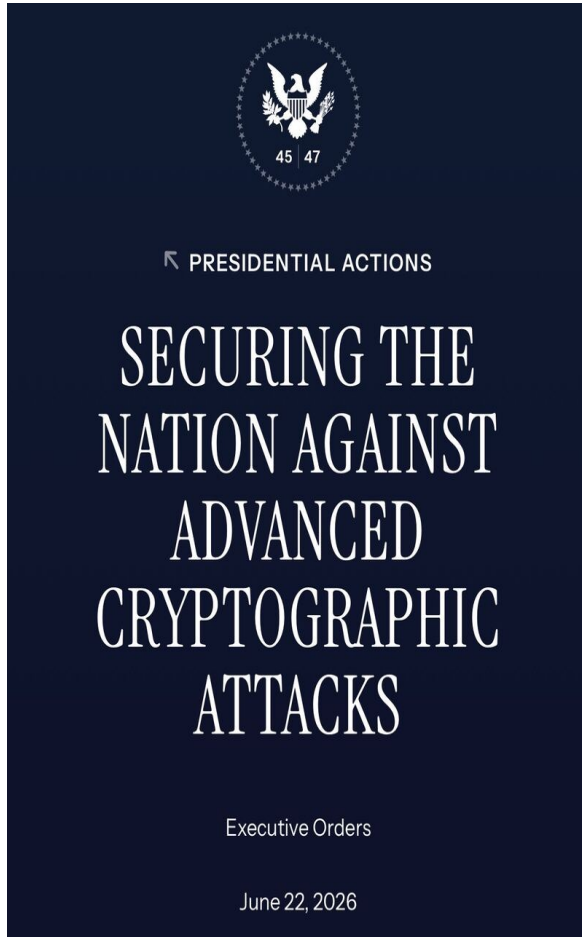
Completare la transizione al PQC per i sistemi ad **alto** rischio

Entro il 31.12.2035



Completare la transizione PQC per i sistemi a **medio** rischio (e il più possibile i sistemi a **basso** rischio)

Executive Order



22.06.2026

Entro il **22/09/2026**:

- L'Office Management and Budget deve emanare una *guidance* per la migrazione PQC delle agenzie federali (**emanato il 24 giugno**).

Entro **24/07/2026**:

- Ogni Agenzia Federale deve nominare un PQC migration Lead

Entro **22/12/2026**:

- Il NIST deve avviare un progetto pilota di migrazione PQC

Entro **31/12/2030**:

- Gli *High Value Assets* devono migrare a PQC per il key establishment

Entro **31/12/2031**:

- Gli *High Value Assets* devono migrare a PQC per firma digitale



**Tempi anticipati
rispetto a
precedenti
indicazioni USA**

ACN coordina questa iniziativa a livello nazionale, **in linea con la European Coordinated Implementation Roadmap**.

In qualità di Autorità nazionale per la cybersicurezza, ACN supporta lo **sviluppo di un approccio nazionale coordinato e basato sul rischio** per la transizione verso la crittografia post-quantistica.

Il ruolo di ACN è quello di **definire un quadro strategico e tecnico comune**, coinvolgere i principali stakeholder pubblici e privati, fornire indirizzi, stabilire priorità e tempistiche a livello nazionale e **monitorare l'avanzamento complessivo** della transizione.

Ciascuna organizzazione resterà responsabile della valutazione della propria esposizione, della pianificazione della migrazione e dell'attuazione delle misure necessarie all'interno dei propri sistemi.

Transizione alla PQC - Linea di azione nazionale



WORK IN
PROGRESS

Pianificazione nazionale

Entro **Ottobre 2026**

Redazione del **primo draft del Piano Nazionale di transizione**

Entro **Novembre 2026**

Coinvolgimento altre istituzioni e settore industriale (fase consultazione)

Entro **Dicembre 2026**

Pubblicazione **Piano Nazionale di transizione**

Entro **Giugno 2027**

Emissione **linee guida operative**

Pianificazione dei soggetti

Entro **2028**

Pianificazione attività di transizione da parte dei soggetti interessati

Esecuzione

Entro **2030**

Completamento attività di transizione per sistemi ad **alto** rischio

Entro **2035**

Completamento attività di transizione per sistemi a **medio** e **basso** rischio

INDIVIDUAZIONE DEI SOGGETTI ESPOSTI

Rappresenta il fulcro per capire il grado di coinvolgimento di un soggetto nell'avviare o meno la transizione.

Fornisce strumenti operativi, tramite **questionari**, che permettono una:

- **Valutazione preliminare di esposizione (pre-assessment)**: fornisce un metodo di valutazione qualitativo per definire il livello di esposizione di un soggetto rispetto al rischio quantistico.
- **Valutazione della maturità organizzativa**: fornisce un metodo per analizzare la capacità organizzativa di un soggetto nell'affrontare un processo di analisi e di realizzazione della transizione post-quantum.
- **Valutazione degli impatti sul business**: fornisce criteri generali per valutare il possibile impatto economico derivante dalla minaccia quantistica.



RACCOMANDAZIONI TECNICHE

Descrive nel dettaglio il processo di transizione e fornisce le raccomandazioni a supporto, includendo tutti i passi che si rendono necessari ad avviare e terminare la transizione.

In particolare, viene posto l'accento su:



- **Struttura organizzativa per la gestione della transizione**
- **Sviluppo di competenze per guidare la transizione**
- **Identificazione asset crittografici**
- **Calcolo del rischio quantistico**
- **Pianificazione delle attività di transizione**
- **Avvio e verifica delle attività di transizione**

Guide operative dedicate.

Pubblicazione 1°
semestre del 2027.

GOVERNANCE NAZIONALE DEL PROCESSO DI TRANSIZIONE

- **Unitarietà dell'indirizzo e chiarezza dei ruoli**

Comunicare obiettivi, priorità e criteri a livello nazionale, assicurando coerenza ai percorsi di transizione dei diversi soggetti.

- **Coordinamento nazionale**

Agevolare un processo di transizione il più possibile uniforme, orientato a mantenere l'interoperabilità dei sistemi e dei servizi.



- **Integrazione nell'architettura esistente**

Valorizzare i meccanismi di raccordo già operanti in materia di cybersicurezza, evitando la duplicazione di strutture.

- **Soggetti coinvolti**

Raggiungere la più ampia platea di soggetti, Perimetro nazionale, della NIS II, ulteriori attori rilevanti per il processo di transizione.

- **Monitoraggio a livello nazionale**

Monitorare lo stato di avanzamento della transizione dei soggetti interessati, con opportune garanzie di riservatezza.

CRYPTO AGILITY

La crypto agility è la capacità di un sistema o di un'infrastruttura di sostituire, aggiornare o riconfigurare rapidamente algoritmi, protocolli, parametri e chiavi crittografiche senza dover riprogettare completamente il sistema.

- **Schema crittografico:** deve essere realizzato in modo tale che sia possibile sostituire una primitiva crittografica con un'altra che svolge le stesse funzioni.
- **Software:** deve essere possibile identificare, isolare e sostituire il componente software responsabile dell'operazione crittografica.
- **Hardware:** L'architettura dovrebbe prevedere l'impiego di hardware in grado di poter gestire la sostituzione degli algoritmi.



Tale capacità è difficilmente ottenibile se non si fissano dei requisiti specifici in fase di progettazione.

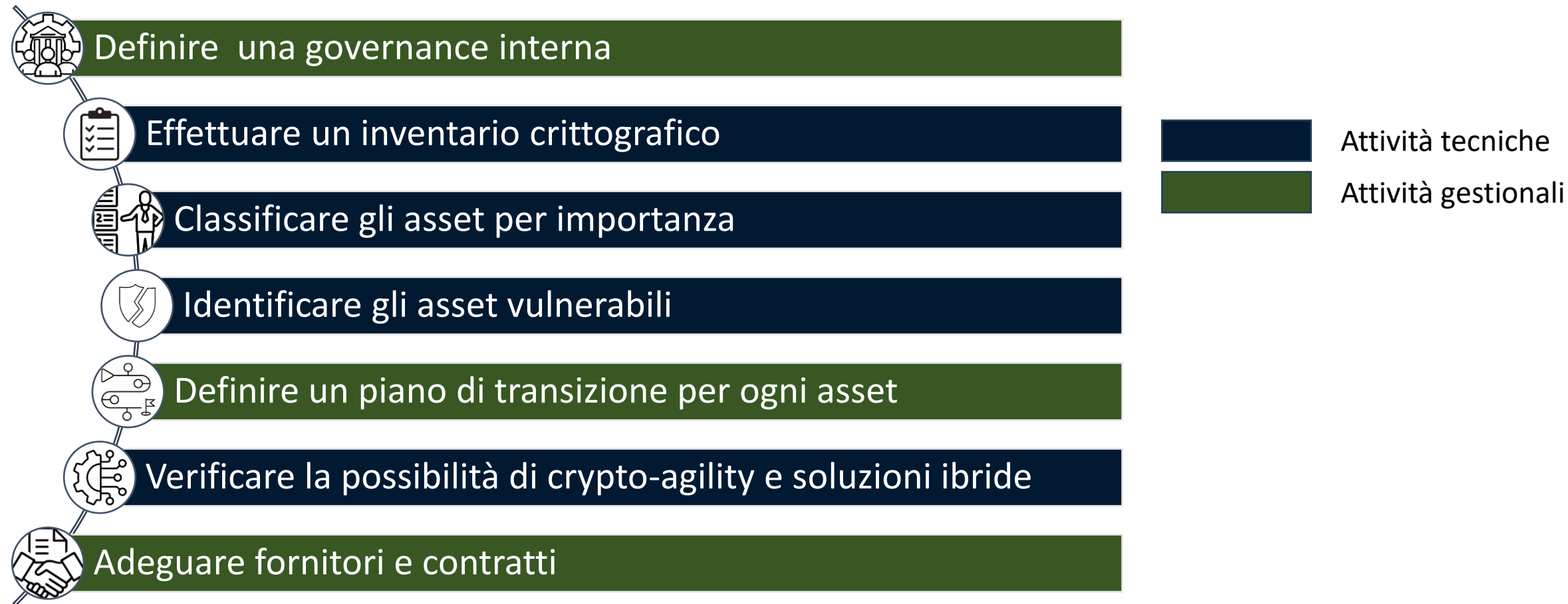
Approfondimenti:

1. Attività necessarie alla transizione dei soggetti esposti
2. Valutazione di maturità organizzativa
3. Cryptoagility

Attività necessarie alla transizione dei soggetti esposti

Ogni SOGGETTO che deve effettuare la transizione dei propri asset deve svolgere una serie di attività.

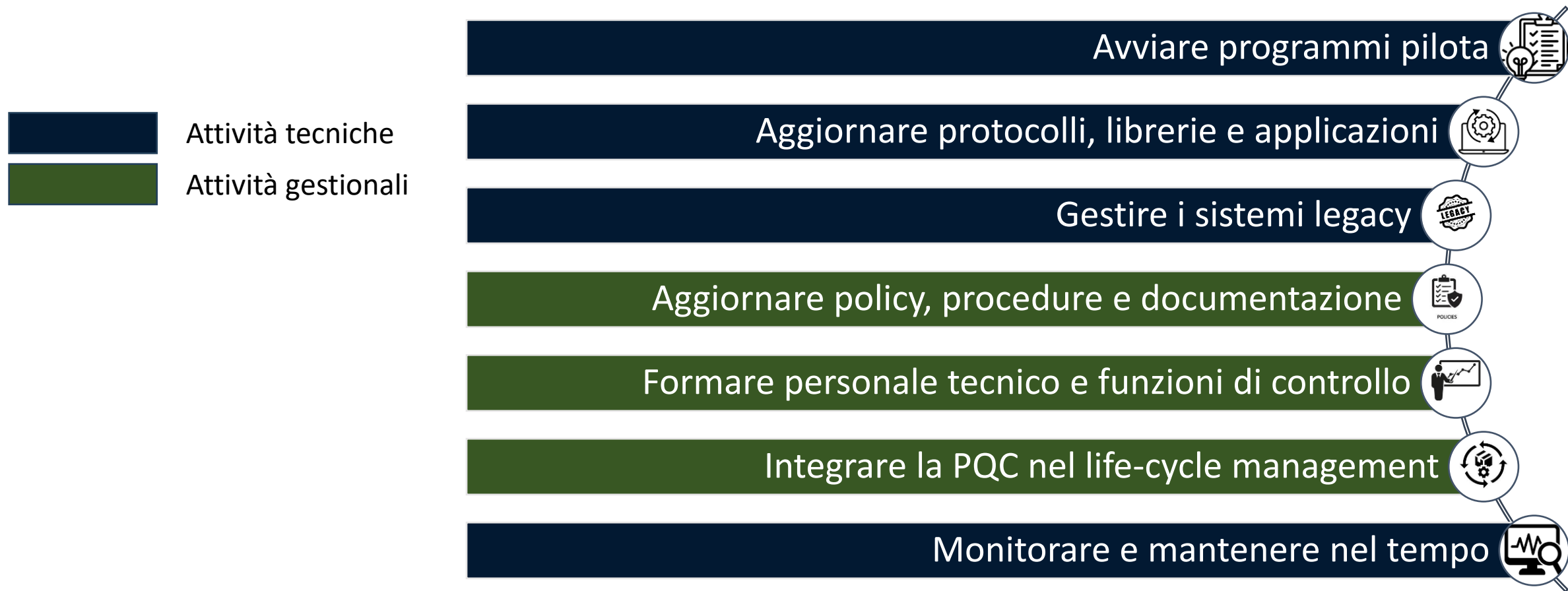
A premessa della transizione



Attività necessarie per la transizione

Ogni SOGGETTO che deve effettuare la transizione dei propri asset deve svolgere una serie di attività.

Durante e dopo la transizione



Valutazione di maturità organizzativa



QUESTIONARIO DI AUTOVALUTAZIONE DELLA MATURITÀ ORGANIZZATIVA

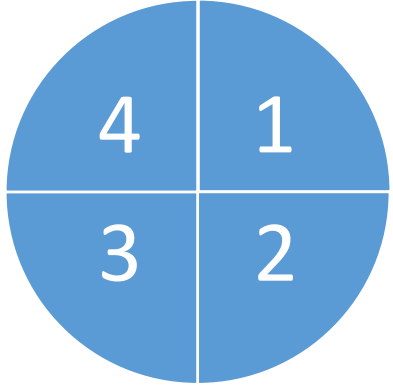
Consente di:

- **comprendere il proprio livello di preparazione** organizzativa per affrontare la transizione;
- **aumentare la consapevolezza** sul percorso di preparazione in vista della transizione;
- **avviare il confronto** tra figure responsabili e **upper management.**

Chief Information Security Officer (CISO)
Chief Information Officer (CIO)
Chief Technology Officer (CTO)
Chief Risk Officer (CRO)
Chief Data Officer (CDO)

Fornisce:

- **indici** di maturità organizzativa;
- **raccomandazioni** per avanzare nel percorso di preparazione in vista della transizione;
- **suggerimenti** sulle aree di intervento prioritarie (anche in base alla natura del soggetto interessato).



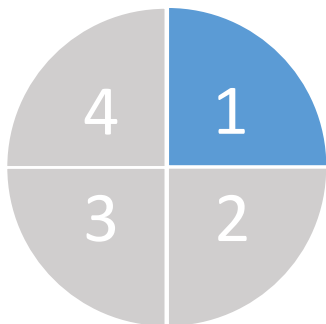
Architettura del questionario suddivisa in **4 Domini**

Per ogni Dominio si individuano degli **Obiettivi**

Per ogni Obiettivo si individuano **5 Livelli di maturità**:

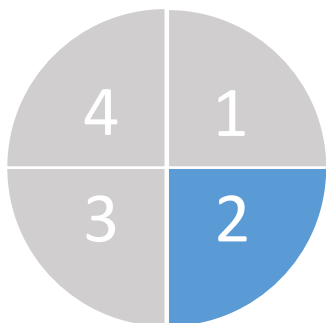


0. Mancano i presupposti per attivarsi verso l'obiettivo;
1. Sussistono i presupposti, ma non è stato ancora conseguito alcun risultato;
2. Sono stati conseguiti i primi risultati parziali;
3. Obiettivo raggiunto, ma una mutazione del contesto potrebbe invalidare i risultati;
4. Obiettivo raggiunto e consolidato mediante un processo di miglioramento continuo.



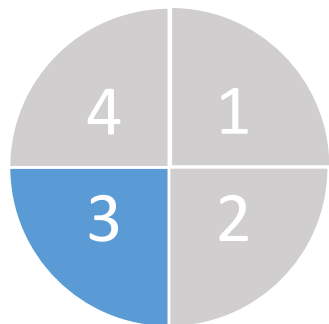
Consapevolezza

- Conoscere la minaccia quantistica per la crittografia e quindi per la cybersicurezza
- Conoscere i principi base della PQC e riconoscere la necessità di migrare verso tale soluzione
- Comprendere il concetto di crypto-agility e la sua importanza per l'efficacia della transizione
- Sapere quali dei servizi e applicazioni utilizzati impiegano la crittografia e a quale scopo



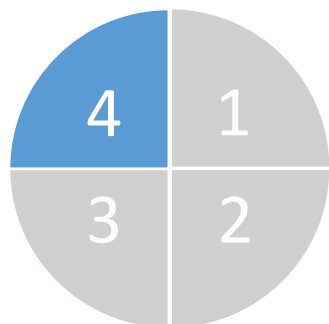
Controllo di filiera e relazioni esterne

- Sapere quali servizi e applicazioni forniti da terzi impiegano la crittografia e a quale scopo
- Conoscere gli usi della crittografia all'interno dei servizi e prodotti realizzati
- Identificare le proprie esigenze di supporto esterno
- Connettersi con l'ecosistema del proprio settore



Gestione del rischio

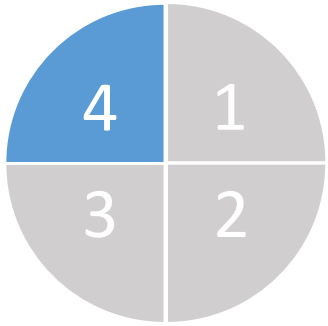
- Gestire continuativamente i rischi di cybersicurezza e il ciclo di vita delle tecnologie
- Integrare la minaccia quantistica nella gestione dei rischi di cybersicurezza



Competenze e Governance

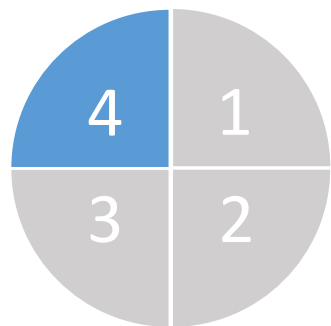
- Dotarsi di personale competente per la gestione della transizione
- Stabilire una struttura di governance formale deputata alla gestione della transizione
- Definire gli obiettivi e le priorità della transizione

N.B.: Anche realtà contenute, o che decidano di affidare larghe parti della transizione in outsourcing, necessitano di una governance appropriata per guidare la transizione.



Competenze e Governance

OBIETTIVO: Stabilire una struttura di governance formale deputata alla gestione della transizione.

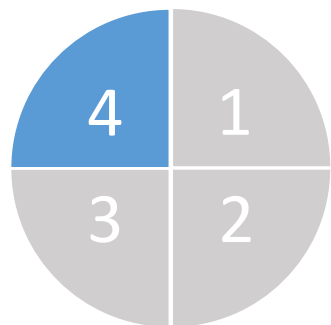


Competenze e Governance

OBIETTIVO: Stabilire una struttura di governance formale deputata alla gestione della transizione.

LIVELLI DI MATURITÀ

0. Non sono state identificate figure responsabili per la transizione.
1. È stato identificato un responsabile per la transizione, ma non sono state assegnate eventuali responsabilità discendenti.
2. Sono state formalmente assegnate tutte le diverse responsabilità, ma non esiste ancora una struttura completa di tutti i ruoli e i gruppi di lavoro necessari o non è stato definito il coordinamento interno.
3. È stata creata una struttura di governance completa, ma non è stato adottato un processo formale di rivalutazione e adattamento periodico della struttura di governance.
4. Esiste una struttura di governance formale per la gestione della transizione, completa di responsabilità, ruoli, gruppi di lavoro e sistema di coordinamento interno; inoltre, esiste un processo di rivalutazione e adattamento periodico della struttura di governance.



Competenze e Governance

OBIETTIVO: Stabilire una struttura di governance formale deputata alla gestione della transizione.

RACCOMANDAZIONI per il Passaggio di Livello

- 0 -> 1. *Individuare e formalizzare una figura responsabile per la transizione, attribuendole il compito di indirizzare e supervisionare le relative attività.*
- 1 -> 2. *Individuare le funzioni organizzative coinvolte nella transizione e assegnare formalmente le relative responsabilità, definendo chiaramente i rispettivi ambiti di competenza.*
- 2 -> 3. *Completare la struttura di governance assegnando i ruoli operativi*, istituendo i gruppi di lavoro necessari* e definendo modalità formali di coordinamento tra le funzioni coinvolte (come riunioni a intervalli regolari, etc.).*
- 3 -> 4. *Definire un processo di riesame periodico della struttura di governance, verificandone l'adeguatezza e adattando ruoli, responsabilità, gruppi di lavoro e meccanismi di coordinamento in funzione dell'avanzamento della transizione e dell'evoluzione del contesto.*

*vedere piano di transizione per indicazioni più dettagliate

Cryptoagility del TLS

A livello di **schema crittografico**, TLS può essere considerato crypto-agile perché **non lega il protocollo a un unico algoritmo crittografico**, ma definisce funzionalità crittografiche astratte che possono essere realizzate con primitive diverse. Questi meccanismi vengono peraltro **negoziati durante l'handshake** tra client e server.



Cipher Suites

TLS 1.3 (suites in server-preferred order)

TLS_AES_256_GCM_SHA384 (0x1302) ECDH x25519 (eq. 3072 bits RSA) FS

TLS_CHACHA20_POLY1305_SHA256 (0x1303) ECDH x25519 (eq. 3072 bits RSA) FS

TLS_AES_128_GCM_SHA256 (0x1301) ECDH x25519 (eq. 3072 bits RSA) FS

TLS 1.2 (suites in server-preferred order)

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) ECDH x25519 (eq. 3072 bits RSA) FS

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) ECDH x25519 (eq. 3072 bits RSA) FS

TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8) ECDH x25519 (eq. 3072 bits RSA) FS

Esempio di *cipher suite* negoziabili da un server durante l'handshake del protocollo TLS.

A **livello software**, le implementazioni TLS sono generalmente predisposte alla crypto-agility, poiché le funzionalità crittografiche sono normalmente demandate a librerie dedicate e aggiornabili (come OpenSSL o analoghe).

In pratica, l'applicazione non deve “conoscere” direttamente RSA, AES, ..., ma dovrebbe affidarsi a una **libreria crittografica** che espone funzioni generiche.

Ciò consente, in molti casi, di introdurre nuovi algoritmi o disabilitare quelli obsoleti intervenendo sulla libreria e sulla configurazione, senza modificare la logica applicativa.

Esempi di *Chiper Suites* negoziate dal Client Chrome con il Server collegato

Chrome 70 / Win 10	-	TLS 1.3	TLS_AES_256_GCM_SHA384 ECDH x25519 FS
Chrome 80 / Win 10	-	TLS 1.3	TLS_AES_256_GCM_SHA384 ECDH x25519 FS
Chrome 131 / Win 10	-	TLS 1.3	TLS_AES_256_GCM_SHA384 PQC X25519MLKEM768 FS

A livello **hardware**, TLS può essere considerato crypto-agile **solo se la piattaforma che esegue le operazioni crittografiche è sufficientemente flessibile.**

In questi casi la crypto-agility dipende dal fatto che tali componenti siano **aggiornabili, programmabili, modulari o facilmente sostituibili.**



Caso semplice

Laptop che usa Google Chrome e hw general purpose



Caso complesso

Dispositivi medicali
connessi con risorse hw
limitate



Transizione nazionale alla crittografia post-quantum

Ancona, 08.10.2026