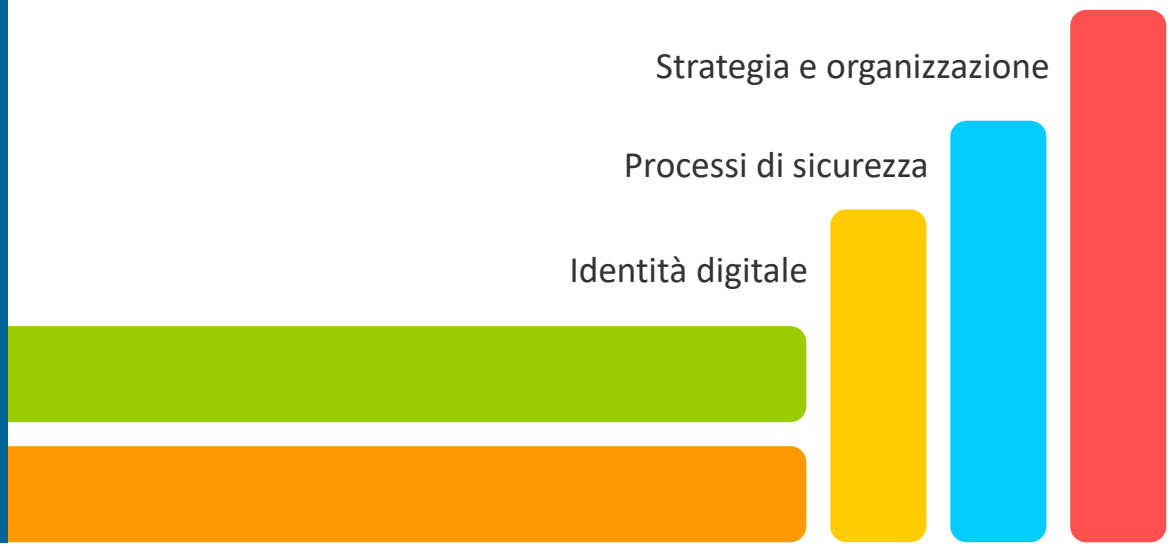
CIPA | Convenzione Interbancaria per l'Automazione

ABI Associazione Bancaria Italiana

Rilevazione sull'IT nel settore bancario italiano

Profili tecnologici e di sicurezza - Edizione 2026

Cyber security nel settore bancario: rischi e nuove minacce



Rapporto sul 2025

CIPA | Convenzione Interbancaria per l'Automazione

ABI Associazione Bancaria Italiana

Rilevazione sull'IT nel settore bancario italiano

Profili tecnologici e di sicurezza - Edizione 2026

Rapporto sul 2025

Cyber security nel settore bancario: rischi e nuove minacce

Ottobre 2026

Rif. RILTEC-2026 – 1

CIPA, 2026

Indirizzo
Banca d'Italia
Dipartimento Informatica
Servizio Soluzioni per il Trattamento dei Dati e la Trasformazione Digitale
Divisione Cooperazione Interbancaria
Centro Donato Menichella
Largo Guido Carli, 1 – 00044 – Frascati (RM)

Email
segcipa@cipa.it

Sito Internet
www.cipa.it

Questo documento è disponibile sul sito internet della CIPA.

Tutti i diritti riservati. È consentita la riproduzione a fini non commerciali, a condizione che venga citata la fonte.

Infografiche: © Canva tramite Canva.com.

Coordinamento del gruppo interbancario	**Banca d'Italia – CIPA**	Paola Paparo
	ABI Lab	Romano Stasi

Membri del gruppo interbancario	**Banca d'Italia – CIPA**	Katia Boria
		Simona Cecchetti
		Fabrizio Crocetti
		Daniela D'Amicis
		Matteo Elia
		Domenico Petrucciani
		Maria Pia Zambelli
	ABI Lab	Giulio Murri
		Marco Rotoloni
	Banca Nazionale del Lavoro	Lucia Boeri
		Virginia Casella
		Carlo Cotroneo
		Mary Elizabeth Rulloda
		Gerardo Tommasiello
	Monte dei Paschi di Siena	Sabrina Ghilardi
		Antonio Greco
		Andrea Pagni
		Mariagrazia Silvestro
	UniCredit	Vincenzo Montanaro
		Sabrina Scanu
		Mirko Serra
	Credito Emiliano – CREDEM	Giovanni Bertoletti
		Sara Giroldi
		Filippo Lati
		Roberto Mercante
		Vanessa Prando
		Gaia Prigionieri
		Francesco Sani
	Mediolanum	Roberta Somati
		Michele Valente
	Intesa Sanpaolo	Gabriele Colombo
		Roberto Guerini
		Corrado Lonati
		Antonio Melina
		Stefano Passoni
	Banca Generali	Roberto Testa
	Deutsche Bank	Christian Altomare
		Franco Colzani
		Gabriele Tizzoni
		Daniela Trovato
	Banca Sella	Roberto Mosca Balma
		Gianluca Frascino
	Banca IFIS	Gianluigi Colesanti
		Laura Quaroni
	Banco di Desio e della Brianza	Luca Dettori
		Matteo Gusmerini
		Andrea Spinelli
	Allianz Bank	Caterina Sperindei
	Cassa Centrale Banca	Federico Andreatta

	Maria De Gennaro
	Giulia Ghezzi
	Mauro Tramacere
Banco BPM	Cristina Cosenza
	Giuseppe Grieco
	Claudio Elio Mariani
Banca Agricola Popolare di Sicilia	Sergio Digrandi
	Michele Floridia
	Giuseppe Mascaro
	Serena Vaturi
	Pietro Venturella
Banca Popolare Pugliese	Giuseppe Nicola Miggiano
BPER Banca	Antonio Dal Moro
	Anna Fumasoni
	Sergio Taramelli
	Adelaide Aurora Tomasi
	Virgilio Tortora
Banca C.R. Asti	Paolo Cerrato
	Marco Stroppiana
	Stefano Vaccaneo
Crédit Agricole Italia	Ersilia Nijole Atorino
	Roberto Maggipinto
	Anselmo Ruta
	Cesare Zuppa
La Cassa di Ravenna	Alessandro Cela
Iccrea Banca	Marco Esposito
	Luca Gioielli
	Marco Giulianis
	Alessandro Rosi
Banca Passadore	Maurizio Ceragno
	Enrico Gelli



Hanno inoltre collaborato	**Banca d'Italia Dipartimento IT**	Walter Arrighetti
		Alessio Pierotti
		Fabio Segatori
		Francesco Taverna
	ABI Lab	Maria Ferrucci
		Mario Trinchera
	Monte dei Paschi di Siena	Valeria Cerbini
	Credito Emiliano – CREDEM	Alessandro Bozzoli
	Deutsche Bank	Omar Chavarria
	Cassa Centrale Raiffeisen dell'Alto Adige	Ivo Martinolli
	Allianz Bank	Paolo Capodivacca
	Cassa Centrale Banca	Alessandro Censi
	Banco BPM	Elena Maria Rivolta
	Banca Agricola Popolare di Sicilia	Lucia Truppia
	Crédit Agricole Italia	Domenico Iuliano

Hanno contribuito alla definizione e revisione dei contenuti del rapporto anche Claudia Piscitelli, Segretario CIPA e Sonia Guida, vice Segretario CIPA.

Presentazione

La “Rilevazione sull’IT nel settore bancario italiano”, curata da CIPA (Convenzione Interbancaria per l’Automazione) e ABI (Associazione Bancaria Italiana), offre ogni anno un contributo di riflessione sugli aspetti economici, organizzativi e tecnologici connessi con l’utilizzo dell’Information and Communication Technology nel settore bancario. Oltre che agli operatori bancari – ai quali vuole fornire elementi di confronto e di riferimento utili per valutazioni funzionali alle scelte in ambito informatico – l’indagine si rivolge a tutti coloro che, a vario titolo, sono interessati a conoscere l’evoluzione dell’IT nel settore creditizio.

La Rilevazione si articola in due distinte indagini pubblicate separatamente.

La prima, dedicata all’esame dei profili economici e organizzativi dell’IT, analizza l’andamento e la ripartizione dei costi e degli investimenti IT, le principali finalità della spesa informatica, l’assetto organizzativo e le modalità di sourcing, le iniziative di innovazione tecnologica, la composizione e la formazione del personale IT.

La seconda, focalizzata in ogni edizione su una specifica tematica, è riservata ai profili tecnologici e di sicurezza ed è rivolta all’analisi delle scelte IT in materia di metodologie, strumenti e tecnologie innovative, utilizzati nel contatto con la clientela, a supporto dei processi interni e all’esame dei connessi aspetti di sicurezza informatica.

Questa edizione della Rilevazione tecnologica è dedicata al tema della cyber security nel settore bancario, analizzando l'evoluzione dei rischi e delle minacce emergenti. L'indagine approfondisce gli aspetti strategici, organizzativi e tecnologici della sicurezza informatica, valutandone il livello di maturità dei principali processi. Particolare attenzione è inoltre riservata all'impatto delle tecnologie emergenti, quali l'Intelligenza Artificiale e il Quantum Computing, sulle strategie e sugli assetti di sicurezza adottati dal settore bancario.

I rapporti delle indagini sono pubblicati sul sito internet della CIPA (www.cipa.it).

La Presidenza della CIPA esprime apprezzamento per il contributo fornito dai gruppi bancari e dalle banche partecipanti alla Rilevazione e ringrazia i componenti del gruppo di lavoro che ha condotto l’indagine e redatto il presente rapporto.

IL PRESIDENTE DELLA CIPA
(Banca d’Italia)

Giuseppe Zingrillo

LA VICEPRESIDENTE DELLA CIPA
(ABI)

Barbara Pelliccione

Sommario

Sintesi **1**

Campione e note metodologiche **5**

Campione dei partecipanti all'indagine 5

Note metodologiche 7

Capitolo 1. Cyber security e aspetti strategici **9**

1.1 Strategia aziendale per la sicurezza informatica della banca 9

1.2 Processi di sicurezza informatica e iniziative progettuali 13

1.3 Collocazione organizzativa delle funzioni di sicurezza 17

Capitolo 2. Aspetti economici e organizzativi **19**

2.1 Costi e investimenti per la sicurezza informatica 19

2.2 Competenze attuali e richieste 20

2.3 Assunzione, formazione e requisiti 24

Capitolo 3. Contesto geopolitico e focus su processi di sicurezza **29**

3.1 Minacce cyber e contesto geopolitico 29

3.2 Focus sui processi di sicurezza 30

3.3 Cyber Threat Intelligence 31

3.4 Processo di Information Sharing 33

3.5 Processo di Security Assessment – Red Teaming 34

3.6 Vulnerability assessment e Patch management 36

3.7 Processo di Digital forensics 37

3.8 Gestione del rischio di terze parti 38

3.9 Integrazione dei processi e tecnologie a supporto 39

3.9.1 Integrazione sicurezza fisica e logica 39

3.9.2 L'Intelligenza Artificiale (IA) 40

3.10 Post Quantum Cryptography 42

3.11 Ulteriori analisi 44

3.11.1 Sicurezza e cloud 44

3.11.2 Strumenti di sicurezza 46

3.11.3 Modalità di autenticazione alla rete aziendale 46

Capitolo 4. Identità digitale **49**

4.1 Adozione e ambiti di utilizzo degli EUDI Wallet 49

4.2 Modelli di sviluppo 53

4.3 Partecipazione a iniziative europee 54

4.4 Modalità di autenticazione nei servizi alla clientela 56

Indice delle figure **59**

EDIZIONE 2026

RILEVAZIONE TECNOLOGICA CIPA

CYBER SECURITY NEL SETTORE BANCARIO: RISCHI E NUOVE MINACCE

IL QUESTIONARIO

- Strategia
- Processi
- Competenze
- IA, quantum computing, cloud
- Identità digitale

36 domande

I RISPONDENTI

20 Gruppi bancari

3 Banche

STRATEGIA DI SICUREZZA

Tra i rispondenti

100% dispone di una strategia formalizzata

91% aggiorna la strategia almeno ogni 3 anni

100% indirizza le tematiche

- *Cyber security*
- *Formazione e awareness*
- *Gestione rischi terze parti*

PROCESSI

Tra i più maturi

- ***Formazione e awareness***
- ***Security Assessment e Testing***

In evoluzione

- ***Information Sharing***
- ***Digital Forensics***

EDIZIONE 2026

RILEVAZIONE TECNOLOGICA CIPA

CYBER SECURITY NEL SETTORE BANCARIO: RISCHI E NUOVE MINACCE

COMPETENZE

Necessità in prospettiva



INTELLIGENZA ARTIFICIALE

Uso più diffuso nei processi:



Monitoraggio e alerting

Cyber Threat Intelligence

IDENTITÀ DIGITALE

8 rispondenti hanno una roadmap per l'utilizzo degli EUDI Wallet

Casi d'uso previsti

Onboarding della clientela

Ambiti di utilizzo previsti (Top 3)

Conti correnti

Bonifici

Monetica



Sintesi

La “Rilevazione sull’IT nel settore bancario italiano – Profili tecnologici e di sicurezza” affronta, in questa edizione, il tema della “Cyber security nel settore bancario: rischi e nuove minacce”, approfondendo gli aspetti strategici, organizzativi e tecnologici della sicurezza informatica, il livello di maturità dei principali processi di sicurezza e l'impatto delle tecnologie emergenti sul settore bancario.

Il campione della Rilevazione è costituito da 20 gruppi bancari e 3 banche singole, che rappresentano complessivamente il 93,1% del totale attivo del settore bancario italiano.

Il primo capitolo esamina gli aspetti strategici. Tutti i rispondenti dichiarano di disporre di una **strategia formalizzata di sicurezza informatica** e 21 su 23 ne prevedono un aggiornamento almeno triennale. Le tematiche maggiormente indirizzate nella strategia sono la Cyber security, la Formazione e Awareness, la Gestione dei rischi legati alle terze parti e la Cyber Resilience. La figura del CISO risulta formalizzata per 17 dei 23 rispondenti. I **principali processi di sicurezza** presentano nel complesso livelli di maturità elevati, con particolare riferimento al Security Assessment e Testing, alla Formazione e Awareness, alla Definizione della normativa di sicurezza interna. Livelli di maturità inferiori sono segnalati per i processi più innovativi o specialistici, quali la Cyber Threat Intelligence, l'Information Sharing e, soprattutto, la Digital forensics. Le iniziative progettuali risultano più frequentemente concentrate nei processi caratterizzati da minore maturità.

Il secondo capitolo è dedicato agli aspetti economici e organizzativi. Oltre l'80% dei rispondenti dispone di una metodologia strutturata per la rilevazione dei costi di sicurezza e quasi tutti prevedono un **budget IT** dedicato sia alla spesa corrente sia agli investimenti. Per circa due terzi del campione il budget destinato alla sicurezza risulta in aumento rispetto all'anno precedente.

Le **competenze specialistiche** presenti nelle principali funzioni di sicurezza mostrano generalmente livelli di copertura medio-alti, con un ulteriore rafforzamento previsto nel biennio 2026-2027 in molteplici ambiti. Le maggiori necessità di competenza riguardano le attività di Red Teaming, le funzioni di Vulnerability Assessment/Penetration Test, il Risk Assessment e l'Incident Response. Il ricorso a risorse esterne rappresenta la modalità prevalente di reperimento delle competenze più specialistiche, in particolare negli ambiti Red Teaming, Digital forensics e Cyber Threat Intelligence. Tra i requisiti richiesti per il personale esperto in sicurezza prevalgono l'esperienza pregressa in specifici ambiti di sicurezza, la conoscenza di normative e standard e il possesso di certificazioni professionali riconosciute a livello internazionale. Le certificazioni maggiormente considerate risultano la CISSP, la CISM e la CISA. Le attività di formazione in materia di sicurezza informatica sono diffuse presso la quasi totalità dei rispondenti e coinvolgono non soltanto il personale tecnico, ma anche il personale amministrativo e di business, l'alta dirigenza e, per alcuni, la clientela e i fornitori.

Il terzo capitolo approfondisce il **contesto geopolitico** e alcuni processi di sicurezza ritenuti particolarmente significativi. Tra le minacce maggiormente considerate nel processo di Risk assessment IT emergono gli attacchi finalizzati all'interruzione dei servizi bancari, il furto di dati

sensibili e le problematiche della catena di fornitura software. Oltre la metà del campione considera anche gli impatti sulla sicurezza derivanti dall'Intelligenza Artificiale e dalle tecnologie quantistiche. Tutti dichiarano inoltre di tenere conto dei rischi connessi al contesto geopolitico in almeno una parte dei propri processi di sicurezza.

Con riferimento alla **Cyber Threat Intelligence (CTI)**, la valutazione della minaccia cyber è ampiamente segnalata: oltre la metà dei rispondenti utilizza tale valutazione nell'ambito dei processi di analisi del rischio, mentre un numero più limitato di banche la integra nei processi di continuità operativa e gestione delle crisi. Sul piano tattico-operativo emerge invece una maturità più elevata, con un significativo impiego delle attività di adattamento dinamico dei presidi di difesa.

L'**Information Sharing** risulta particolarmente sviluppato: quasi tutte le banche partecipano a iniziative di condivisione delle informazioni sulle minacce informatiche, prevalentemente attraverso iniziative nazionali e, in diversi casi, anche internazionali.

Le attività di **Security Assessment - Red Teaming** risultano eseguite o previste da quasi tutti i rispondenti. La maggior parte delle banche dichiara di aver già svolto tali esercizi e di prevederne l'esecuzione periodica.

Anche il processo di **Vulnerability Assessment e Patch Management** evidenzia livelli elevati di maturità: la grande maggioranza dei rispondenti effettua la prioritizzazione delle vulnerabilità considerando congiuntamente criticità, sfruttabilità ed esposizione. Risulta invece ancora limitata la diffusione di policy formalizzate di “forensic readiness”, presenti solo presso una parte minoritaria del campione.

Con riferimento alla **Gestione del rischio delle terze parti**, emerge un'elevata diffusione di strumenti di monitoraggio automatizzato, applicati in particolare ai fornitori critici. Si osserva inoltre una progressiva integrazione tra il monitoraggio della sicurezza logica, dei dispositivi IoT e della sicurezza fisica e ambientale, destinata a rafforzarsi ulteriormente nel biennio 2026-2027.

L'utilizzo dell'**Intelligenza Artificiale** nei processi di sicurezza risulta ancora concentrato in alcuni ambiti specifici, tra cui il Monitoraggio e Alerting e la Cyber Threat Intelligence, ma le previsioni indicano una significativa estensione dell'adozione nel prossimo biennio.

Per quanto riguarda la **Post Quantum Cryptography**, le iniziative attuali risultano ancora limitate, ma si prevede una forte crescita delle attività di analisi del parco applicativo, di crypto agility e di adozione di algoritmi quantum-safe.

Le ulteriori analisi evidenziano una diffusa **adozione di strumenti di base per la sicurezza** quali CMDB, SIEM, piattaforme di Vulnerability Assessment e sistemi di detection e response. In ambito **cloud** le banche tendono a mantenere internamente il presidio delle attività di monitoraggio e gestione degli accessi, ricorrendo invece ai cloud provider per le funzionalità più strettamente integrate con l'infrastruttura. Le modalità di autenticazione alla rete aziendale evidenziano una crescente diffusione di meccanismi di autenticazione multi-fattore sia per i dipendenti sia per le terze parti.

Il quarto capitolo è dedicato all'identità digitale. Quasi un terzo dei 23 rispondenti ha già definito una roadmap per l'adozione degli **EUDI Wallet**, destinati principalmente ai processi di onboarding della clientela. Gli ambiti di utilizzo maggiormente indicati riguardano i conti correnti, i bonifici e la monetica. Le **Attestazioni Elettroniche di Attributi (EAA)** suscitano interesse soprattutto per informazioni provenienti dall'Anagrafe e dalle Entità finanziarie. Le banche che stanno sviluppando soluzioni in questo ambito privilegiano modelli che combinano ricorso a risorse interne ed esterne.

Risulta ancora limitata la partecipazione a **iniziative europee** dedicate all'ecosistema degli EUDI Wallet e marginale l'interesse verso l'utilizzo della DLT per tali soluzioni.

Con riferimento alle **modalità di autenticazione della clientela**, il 2025 continua a essere caratterizzato dall'utilizzo prevalente di meccanismi tradizionali basati su password, fattore biometrico e sistemi OTP. Emergono tuttavia i primi segnali di adozione delle identità digitali conformi al Regolamento UE/2024/1183 (Electronic Identification, Authentication and Trust Services, eIDAS2), la cui diffusione è prevista in significativa crescita nel biennio 2026-2027.

L'ambito applicativo che suscita il maggiore interesse per tali strumenti è quello dell'**onboarding della clientela**, contesto nel quale si prevede il più esteso impiego delle future soluzioni europee di identità digitale.

Campione e note metodologiche

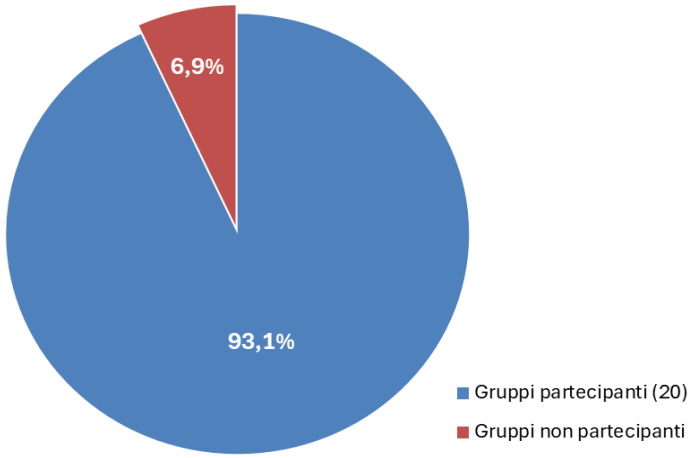
La “Rilevazione sull’IT nel settore bancario italiano – Profili tecnologici e di sicurezza” affronta, in questa edizione il tema della cyber security nel settore bancario considerando i rischi e le nuove minacce, analizzando la maturità e lo stato dell’arte nel settore bancario.

In particolare, il primo capitolo analizza gli aspetti strategici della sicurezza informatica, approfondendo le strategie adottate dai rispondenti, le principali tematiche indirizzate, le iniziative progettuali avviate e gli assetti organizzativi delle funzioni di sicurezza. Il secondo capitolo è dedicato agli aspetti economici e organizzativi, esaminando costi, investimenti, competenze, modelli organizzativi e formazione. Gli aspetti tecnologici ed evolutivi della sicurezza sono trattati nel terzo capitolo, che approfondisce processi, strumenti e tecnologie innovative, tra cui Intelligenza Artificiale, sicurezza del cloud e crittografia post-quantistica. Il quarto capitolo è dedicato all'identità digitale e analizza gli EUDI (European Digital Identity) Wallet, le attestazioni elettroniche di attributi e le prospettive evolutive dei sistemi di autenticazione nel settore bancario.

Campione dei partecipanti all'indagine

Ha aderito all’indagine un campione di 23 rispondenti composto da 20 gruppi - selezionati fra i primi gruppi bancari per totale attivo - e tre banche singole, denominati nel seguito rispondenti o banche. I gruppi partecipanti alla Rilevazione rappresentano il 93,1% dell’insieme dei gruppi bancari in termini di totale attivo[1] (Figura 1).

Figura 1 – Rappresentatività del campione dei gruppi per totale attivo



[1] Il totale attivo considerato al 31.12.2025 fa riferimento al gruppo bancario, comprensivo di tutte le sue componenti (bancarie e non bancarie) soggette a normativa prudenziale (es. banche, società strumentali, società finanziarie, SIM, filiali estere) secondo le segnalazioni di vigilanza consolidata.

Il campione dei gruppi, in base alla classificazione per dimensione operativa[2], risulta composto da: 6 gruppi Principali, 7 gruppi Medi e 7 gruppi Piccoli. L'elenco dei gruppi e delle banche partecipanti è riportato in Tabella 1.

Tabella 1 – Gruppi bancari e banche partecipanti alla Rilevazione

	6 gruppi Principali
1030	Gruppo Monte dei Paschi di Siena
2008	Gruppo UniCredit
3069	Gruppo bancario Intesa Sanpaolo
5034	Gruppo Banco BPM
5387	Gruppo BPER Banca
8000	ICCREA Banca
	7 gruppi Medi
1005	Gruppo bancario Banca Nazionale del Lavoro
3032	Gruppo Credito Emiliano – CREDEM
3062	Gruppo bancario Mediolanum
3104	Gruppo Deutsche Bank
3311	Gruppo Sella
3599	Cassa Centrale Banca
6230	Gruppo bancario Crédit Agricole Italia
	7 gruppi Piccoli
3075	Banca Generali
3205	Banca IFIS
3440	Gruppo Banco di Desio e della Brianza
3589	Allianz Bank
5036	Gruppo bancario Banca Agricola Popolare di Sicilia
6085	Gruppo Cassa di Risparmio di Asti
6270	Gruppo La Cassa di Ravenna
	3 Banche singole
3332	Banca Passadore & C.
3493	Cassa Centrale Raiffeisen dell'Alto Adige
5262	Banca Popolare Pugliese

[2] Le classi dimensionali dei gruppi sono definite come segue:
- **Principali** totale attivo > 120 miliardi di euro;
- **Medi** totale attivo > 20 miliardi e ≤ 120 miliardi di euro;
- **Piccoli** totale attivo ≥ 5 miliardi ≤ 20 miliardi di euro.

Note metodologiche

L'indagine è basata su un questionario predisposto dalla Segreteria Tecnica della CIPA con la collaborazione del gruppo di lavoro interbancario e pubblicato sul sito Internet della CIPA (www.cipa.it) somministrato nel 2025; i dati sono stati acquisiti tramite la piattaforma Sondaggi della Banca d'Italia, e si riferiscono, nella situazione attuale, al 2025 e, in quella prospettica, al 2026-2027.

Nella Rilevazione si fa riferimento alla realtà bancaria all'interno del perimetro nazionale. Per i gruppi si considerano le componenti bancarie e le società strumentali, IT e non IT, che operano a supporto dell'attività bancaria (c.d. perimetro CIPA).

Le percentuali di partecipanti all'indagine indicate nelle rappresentazioni grafiche ("% di rispondenti") sono calcolate rapportando il numero di coloro che forniscono almeno una risposta alla domanda da cui è tratto il grafico al totale dei partecipanti. In alcune analisi, laddove un singolo rispondente può fornire più risposte associate a uno stesso item, viene riportata l'indicazione "risposte multiple".

Capitolo 1. Cyber security e aspetti strategici

Il primo capitolo esamina gli aspetti strategici della sicurezza informatica nel settore bancario, anche con riferimento alla cyber security, intesa come ambito della sicurezza informatica focalizzato sulla protezione di reti, sistemi, applicazioni e dati dalle minacce provenienti dal cyber spazio, incluse attività malevole, attacchi informatici, compromissioni e interruzioni operative.

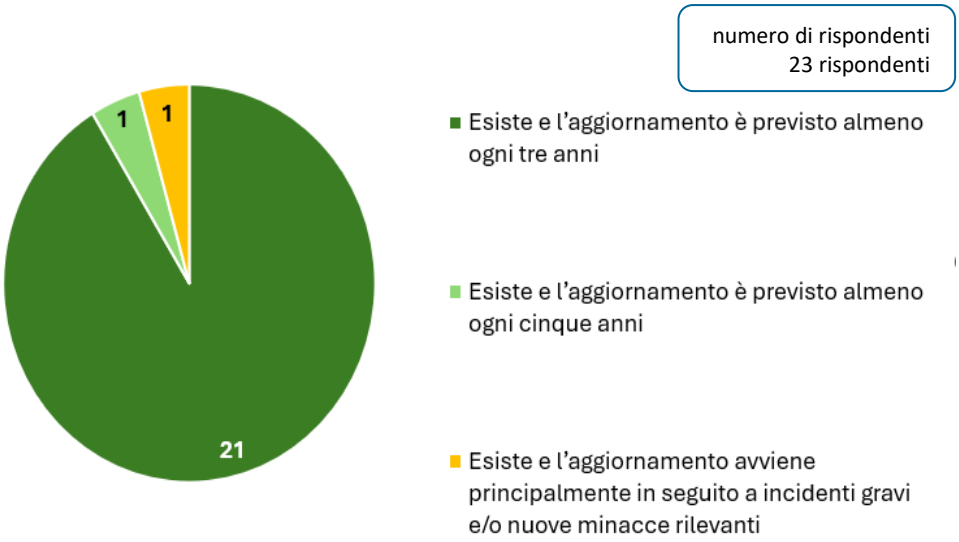
Dopo aver analizzato le principali caratteristiche della strategia aziendale per la sicurezza informatica, anche in relazione alla cyber security e all'Intelligenza Artificiale, il capitolo evidenzia il livello di maturità dichiarato dai rispondenti nei principali processi di sicurezza e le iniziative progettuali avviate nei diversi ambiti considerati.

1.1 Strategia aziendale per la sicurezza informatica della banca

In questo paragrafo vengono esaminate l'esistenza della strategia aziendale per la sicurezza informatica della banca, le tematiche in essa indirizzate e le figure coinvolte nella sua definizione.

Domanda: *Indicare se è stata definita e approvata una strategia aziendale per la sicurezza informatica e se viene aggiornata periodicamente*.

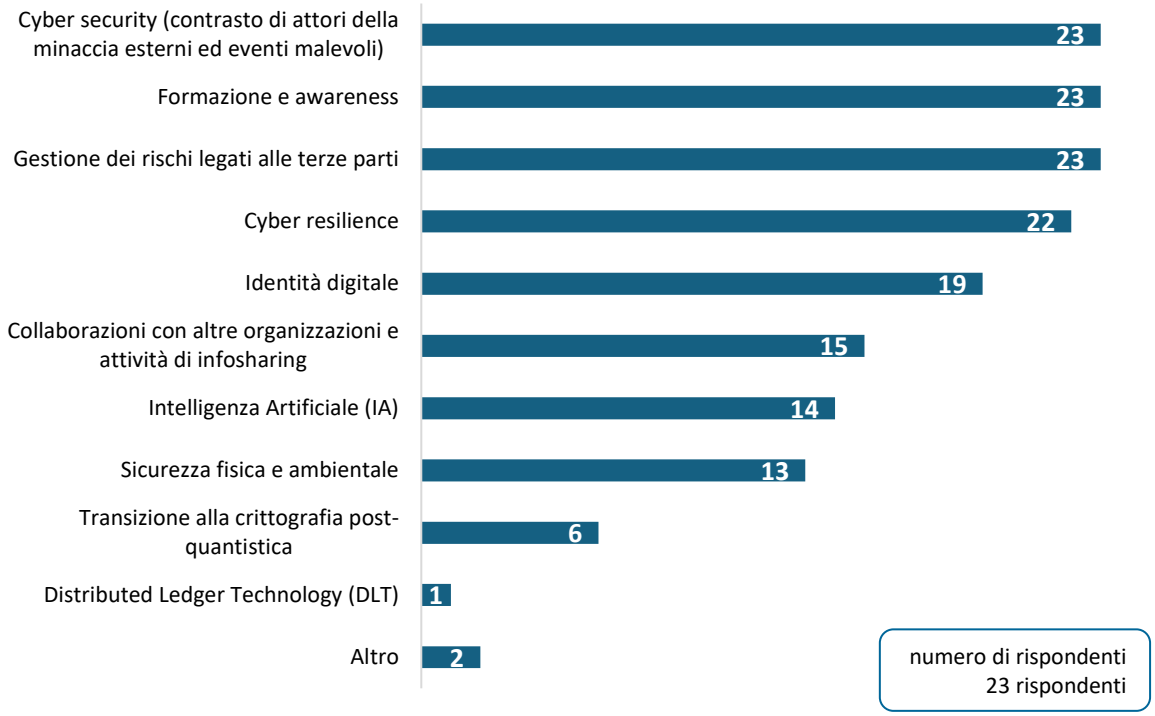
Figura 2 – Strategia aziendale per la sicurezza informatica



Si osserva che al 2025 la totalità delle banche rispondenti dichiara di disporre di una strategia formalizzata di sicurezza informatica. Per 21 banche l'aggiornamento è previsto almeno ogni tre anni, a conferma dell'elevata attenzione rivolta alla governance della sicurezza e all'evoluzione del quadro delle minacce. Solo un numero esiguo di banche prevede revisioni con periodicità ogni cinque anni (1) o in seguito a incidenti gravi e/o all'emergere di nuove minacce rilevanti (1) (Figura 2).

Domanda: *Indicare quali delle seguenti tematiche sono attualmente indirizzate all'interno della strategia per la sicurezza informatica della banca/gruppo bancario.*

Figura 3 – Tematiche di sicurezza indirizzate nella strategia

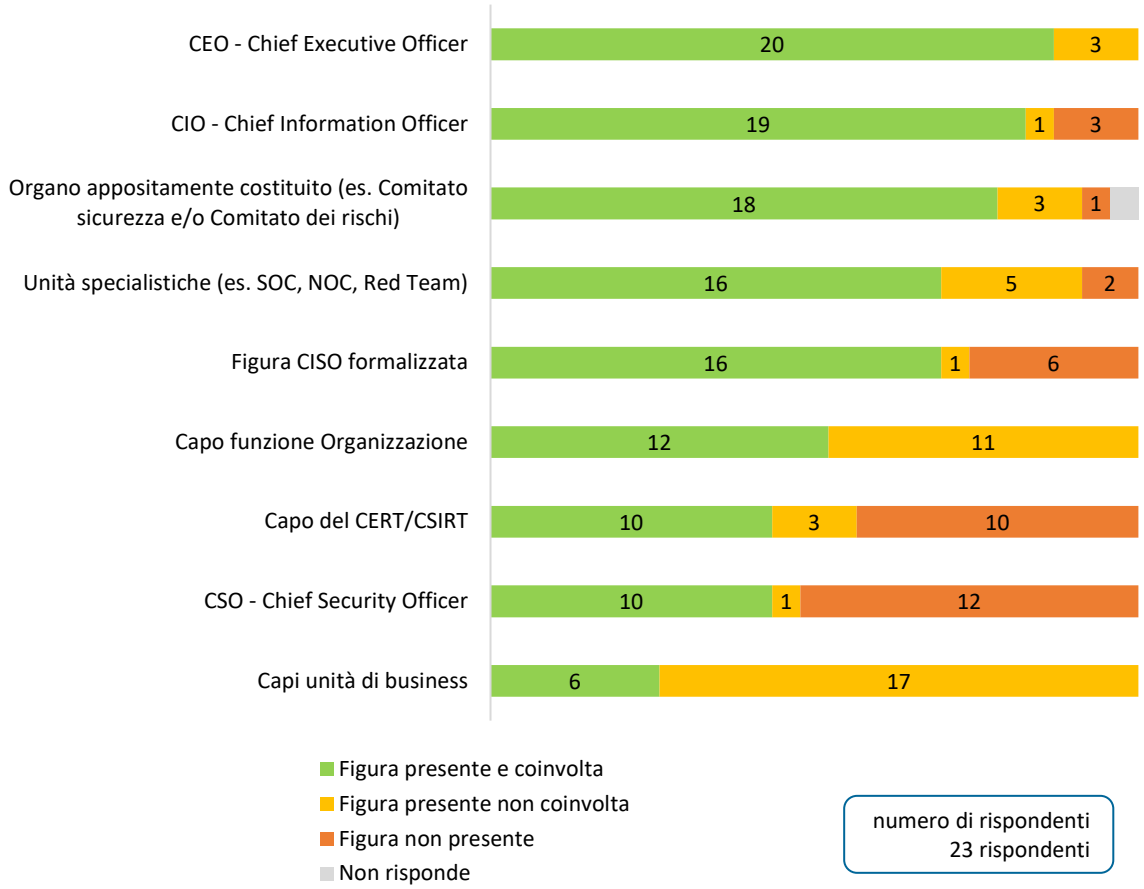


Le tematiche maggiormente indirizzate nella strategia aziendale di sicurezza informatica dal settore bancario sono la Cyber security, la Formazione e awareness e la Gestione dei rischi legati alle terze parti, dichiarate da tutte le banche rispondenti (23). Elevata attenzione è rivolta alla Cyber resilience (22), a conferma del crescente interesse assunto dalla continuità operativa, anche in relazione alla risposta alla normativa europea (cfr. Box 2). Oltre quattro rispondenti su cinque segnalano, tra le tematiche indirizzate dalle loro strategie, l'Identità digitale (19) in considerazione dell'evoluzione dei meccanismi di autenticazione e gestione delle identità previsti dal Regolamento UE/2024/1183 (Electronic Identification, Authentication and Trust Services, eIDAS2) (cfr. Cap. 4).

Risultano inoltre ampiamente trattate nella strategia le tematiche di Collaborazione con altre organizzazioni e le attività di infosharing (15) e l'Intelligenza Artificiale (14). Meno ricorrente invece, la Transizione alla crittografia post-quantistica (6) e quasi assente la Distributed Ledger Technology (DLT) (1) (Figura 3).

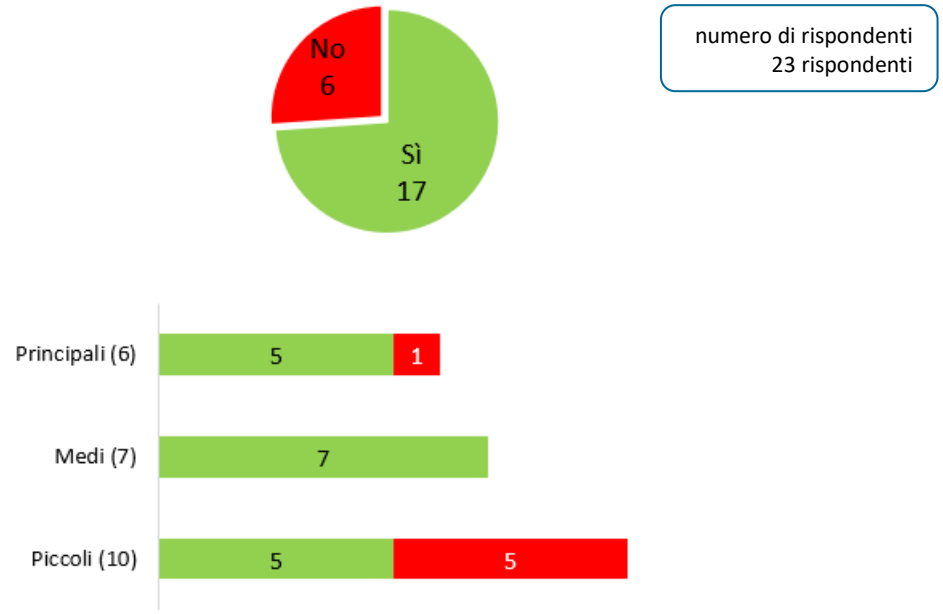
Domanda: *Specificare per tutte le figure elencate il coinvolgimento nella definizione della strategia della sicurezza informatica della banca/gruppo.*

Figura 4 – Figure coinvolte nella definizione della strategia di sicurezza



Dall'analisi della Figura 4 emerge un'ampia partecipazione dei vertici aziendali alla definizione della strategia, a testimonianza della crescente rilevanza della sicurezza nei processi di governo delle banche e del crescente interesse verso tale tematica da parte dell'alta direzione. La maggior parte dei rispondenti coinvolge, nella definizione della strategia, il CEO - Chief Executive Officer (20 rispondenti), il CIO - Chief Information Officer (19), gli Organi appositamente costituiti (es. Comitato sicurezza e/o Comitato dei rischi) (18). D'altra parte, anche le Unità specialistiche (es. SOC, NOC, Red Team), così come il CISO, risultano coinvolti per oltre i due terzi dei rispondenti (16). In misura minore sono presenti livelli di coinvolgimento del Capo funzione Organizzazione (12), il CSO - Chief Security Officer (10), il Capo del CERT/CSIRT (10) e i Capi unità di business (6).

Figura 5 – Figura CISO formalizzata



La figura del CISO è formalizzata per 17 rispondenti su 23.

Si noti che la formalizzazione del CISO risulta particolarmente diffusa tra i rispondenti di media dimensione, che ne dichiarano la presenza nella totalità dei casi, e tra i rispondenti principali (5 su 6). Tra i rispondenti piccoli (che includono le banche singole) si osserva invece la formalizzazione del CISO per la metà del campione (5) (Figura 5).

Box 1 - Chief Information Security Officer (CISO)

Il Chief Information Security Officer (CISO) è la figura responsabile dell'indirizzo, del coordinamento e della supervisione delle attività di sicurezza informatica all'interno dell'organizzazione. Nel tempo, il ruolo del CISO ha assunto una crescente rilevanza strategica, evolvendo da funzione prevalentemente tecnica a presidio di governo dei rischi cyber e della resilienza operativa.

L'importanza del CISO è strettamente collegata al crescente impatto che gli incidenti di sicurezza possono avere sulla continuità operativa, sul patrimonio informativo, sulla reputazione e sul rispetto degli obblighi normativi. Per tale motivo, nelle organizzazioni più mature il CISO opera in stretto raccordo con il vertice aziendale e con le funzioni di gestione del rischio, contribuendo alla definizione delle strategie di sicurezza e alla valutazione dei rischi informatici.

L'efficacia del ruolo del CISO non dipende esclusivamente dalla sua formalizzazione, ma anche dal grado di autonomia, dalle responsabilità attribuite, dalla disponibilità di risorse dedicate e dalla capacità di interagire con gli organi decisionali dell'organizzazione.

In tale prospettiva, il CISO rappresenta un elemento di raccordo tra le esigenze di sicurezza informatica, gli obiettivi di business e i requisiti di conformità normativa, contribuendo alla diffusione di una visione integrata del rischio cyber all'interno dell'organizzazione.

Fonti

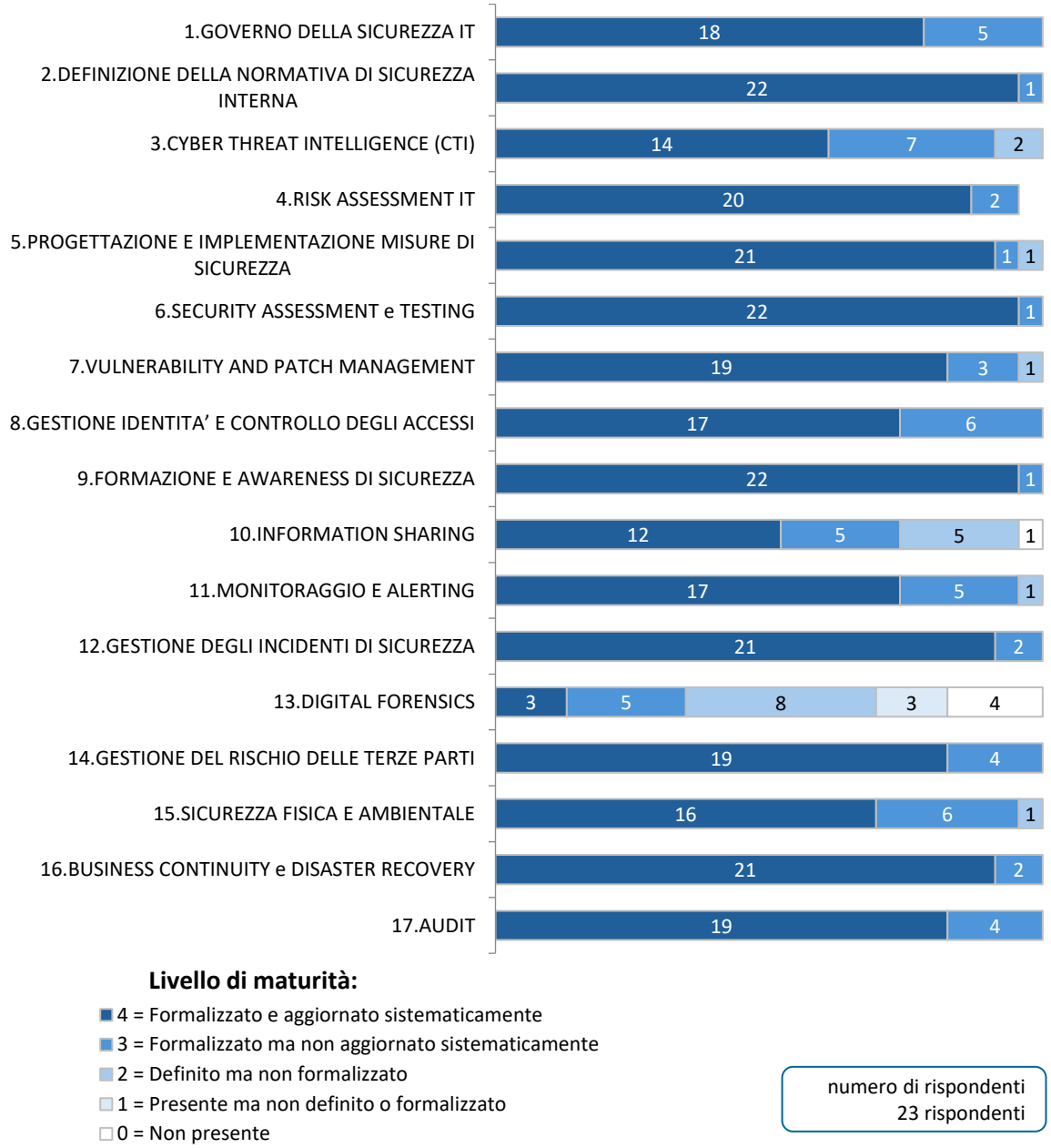
NIST, Workforce Framework for Cyber security (NICE Framework)
https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center
ENISA, Cyber security Skills Framework (ECSF)
https://www.enisa.europa.eu/topics/cybersecurity-education/european-cybersecurity-skills-framework
European Banking Authority (EBA), Guidelines on ICT and security risk management
https://www.eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-ict-and-security-risk-management

1.2 Processi di sicurezza informatica e iniziative progettuali

Nel secondo paragrafo vengono analizzati i processi di sicurezza informatica e le iniziative progettuali in essi avviate dai rispondenti. I processi considerati sono stati individuati sulla base dei principali standard, framework e linee guida in materia di sicurezza informatica e sono stati integrati da specifici sottoprocessi riferiti ad ambiti particolarmente innovativi o in fase di evoluzione, quali la Cyber Threat Intelligence (CTI), la Digital forensics e l'Information Sharing.

Domanda: *In considerazione dei principali processi di sicurezza elencati, specificare il relativo livello di maturità e indicare se la banca/gruppo ha avviato iniziative di tipo progettuale.*

Figura 6 – Livello di maturità e iniziative progettuali nei processi di sicurezza



I risultati mostrano un elevato livello di maturità nei principali processi di sicurezza informatica: per gran parte degli ambiti considerati, la maggioranza dei rispondenti dichiara infatti processi formalizzati e aggiornati sistematicamente.

In particolare, quasi tutti indicano il livello di maturità più elevato nella Definizione della normativa di sicurezza interna, nelle attività di Security Assessment e Testing e nella Formazione e Awareness di sicurezza (22). La formalizzazione e l'aggiornamento sistematico si registra anche per i processi di Progettazione e implementazione delle misure di sicurezza, Gestione degli incidenti di sicurezza, Business continuity e disaster recovery (21) e Risk assessment IT (20).

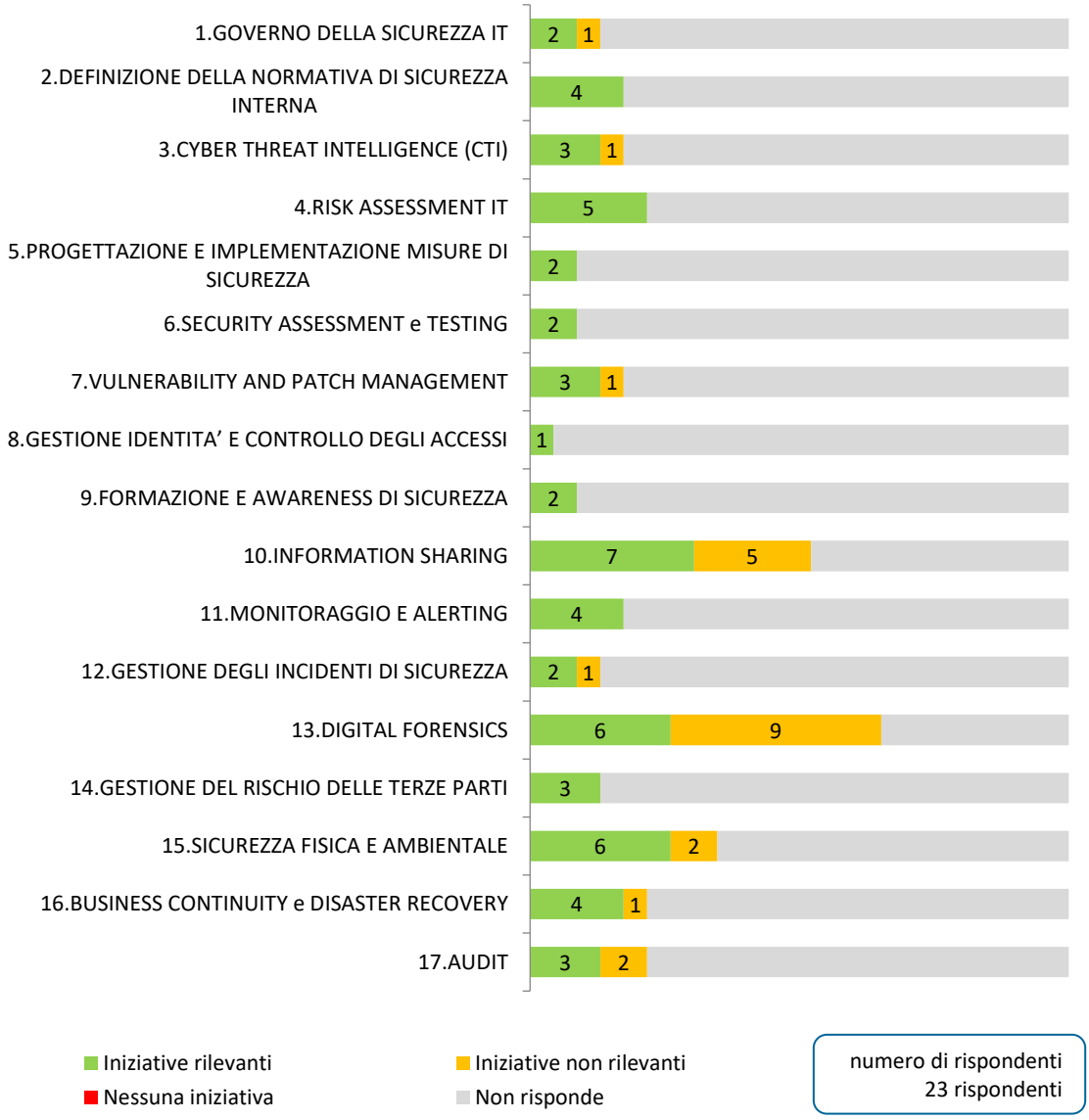
Il livello di maturità più elevato si ha per 19 rispondenti in relazione al Vulnerability and Patch management, la Gestione del rischio delle terze parti e l'Audit.

Sono dichiarati invece meno maturi i processi più innovativi o in fase di evoluzione. In particolare, la Cyber Threat Intelligence (CTI) risulta formalizzata e aggiornata sistematicamente per 14 rispondenti e l'Information Sharing per 12.

Il processo con il livello di maturità più contenuto è la Digital forensics, per il quale soltanto tre rispondenti dichiarano un processo formalizzato e aggiornato sistematicamente (Figura 6).

Domanda: *Indicare se negli ambiti elencati la banca/gruppo ha avviato iniziative di miglioramento della sicurezza informatica o intende avviarle nel biennio 2026-2027, specificandone in prevalenza lo stato.*

Figura 7 – Iniziative progettuali nei processi di sicurezza



In generale, le iniziative progettuali tendono a concentrarsi nei processi che presentano livelli di maturità inferiori. In particolare, un numero elevato di banche segnalano iniziative rilevanti nei processi di Information Sharing (7), Digital forensics (6) e Sicurezza fisica e ambientale (6).

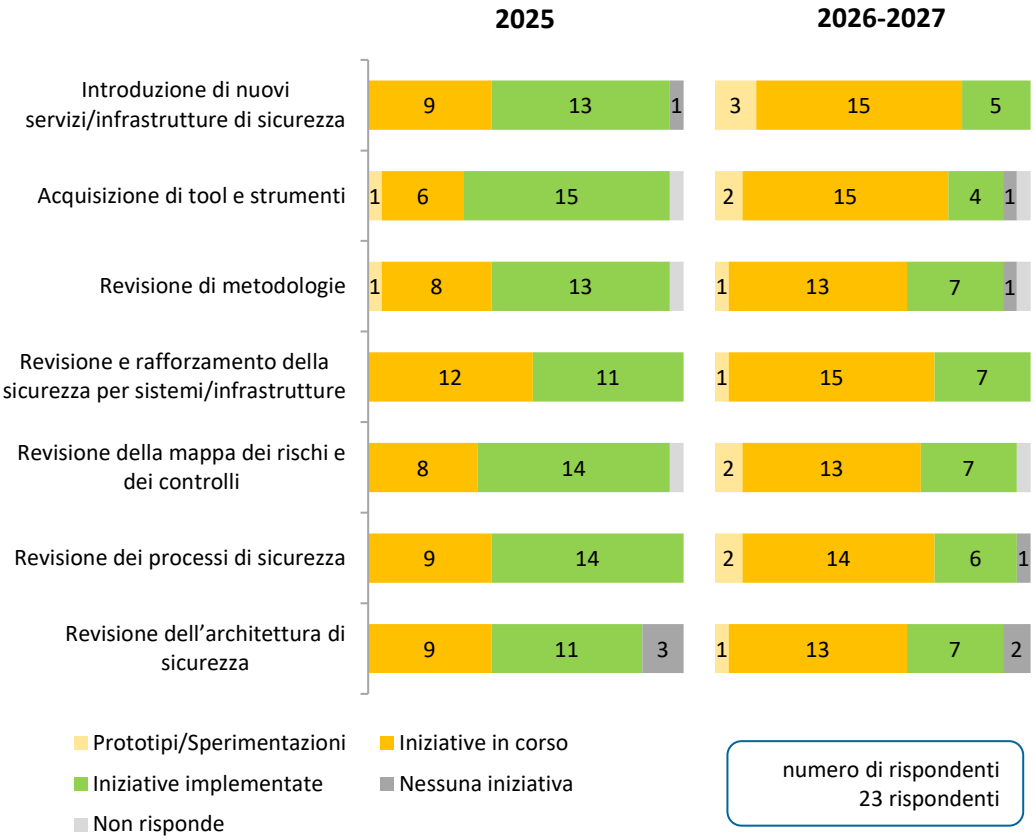
Un numero significativo di banche indicano iniziative rilevanti nei processi di Risk assessment IT (5), Monitoraggio e alerting, Definizione della normativa di sicurezza interna e Business continuity e disaster recovery (4).

D'altra parte, i processi caratterizzati dai livelli di maturità più elevati presentano meno segnalazioni di iniziative progettuali: la Progettazione e implementazione delle misure di sicurezza, il Security assessment e testing, la Formazione e awareness di sicurezza (2), la Gestione delle identità e controllo degli accessi (1) (Figura 7).

Al fine di comprendere meglio le caratteristiche delle iniziative avviate dai rispondenti, l'indagine ha inoltre approfondito le principali tipologie di intervento previste nell'ambito del miglioramento della sicurezza informatica.

Domanda: *Indicare se negli ambiti elencati la banca/gruppo ha avviato iniziative di miglioramento della sicurezza informatica o intende avviarle nel biennio 2026-2027, specificandone in prevalenza lo stato.*

Figura 8 – Tipologie di iniziative



Le iniziative progettuali risultano diffuse in tutti gli ambiti considerati. Già nel 2025 la maggior parte delle banche dichiara di avere in corso o di aver implementato iniziative relative all'Acquisizione di tool e strumenti (6 e 15), alla Revisione dei processi di sicurezza (9 e 14), alla Revisione della mappa dei rischi e dei controlli (8 e 14), all'Introduzione di nuovi servizi/infrastrutture di sicurezza (9 e 13).

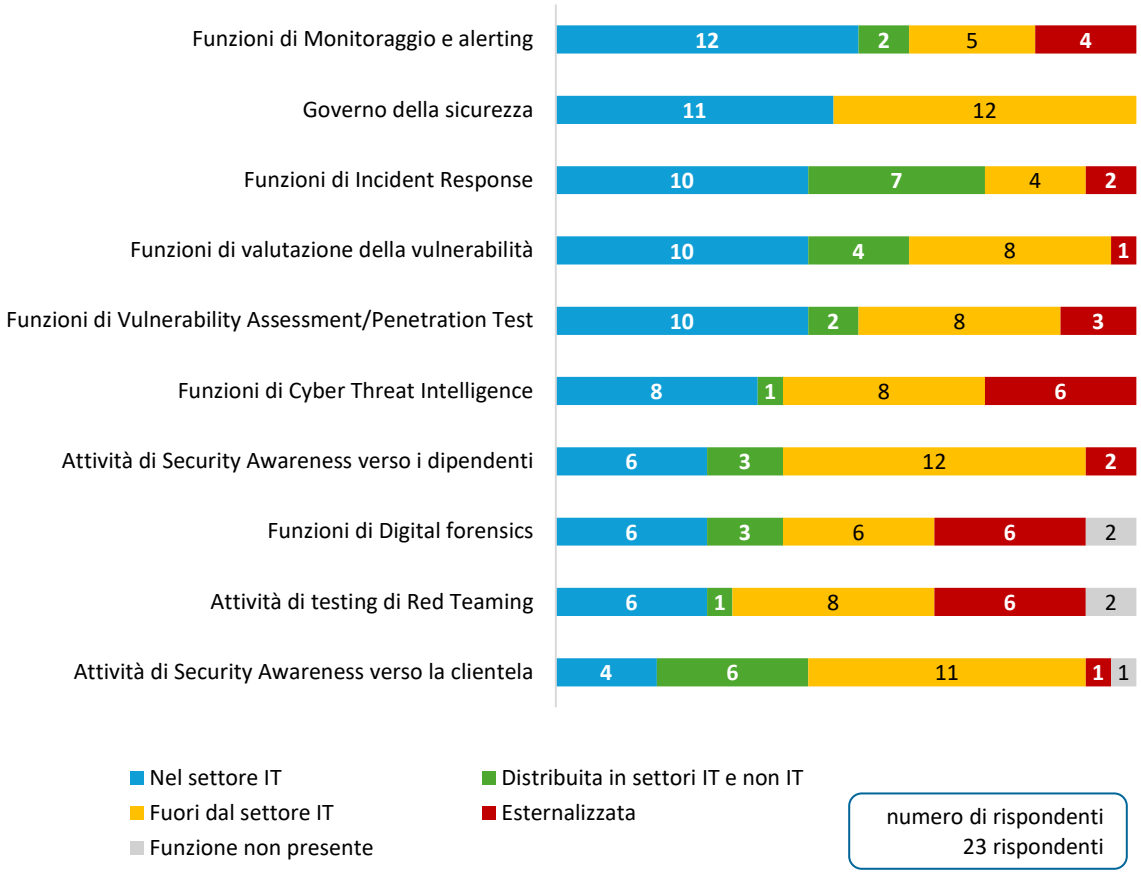
Nel biennio 2026-2027 i rispondenti dichiarano iniziative in corso soprattutto nella Revisione e rafforzamento della sicurezza per sistemi/infrastrutture, nell'Introduzione di nuovi servizi/infrastrutture di sicurezza, nell'Acquisizione di tool e strumenti (15) e sulla Revisione dei processi di sicurezza (14) (Figura 8).

1.3 Collocazione organizzativa delle funzioni di sicurezza

L'indagine prosegue analizzando la collocazione organizzativa delle funzioni di sicurezza, al fine di comprendere in quali ambiti della struttura aziendale siano prevalentemente inserite e in quale misura siano svolte internamente o esternalizzate.

Domanda: *Indicare la collocazione organizzativa delle seguenti funzioni di sicurezza.*

Figura 9 – Collocazione organizzativa delle funzioni di sicurezza



In generale, i risultati evidenziano come le attività maggiormente operative e tecnologiche tendano a essere collocate nel settore IT, mentre le funzioni con una maggiore componente di governo e sensibilizzazione sulla sicurezza risultino più frequentemente distribuite o collocate al di fuori del settore IT.

Infatti, nel settore IT sono più spesso collocate le Funzioni di Monitoraggio e alerting (12), le Funzioni di Incident Response, le Funzioni di valutazione della vulnerabilità e le Funzioni di Vulnerability Assessment/Penetration Test (10). Fuori del settore IT si osservano invece le Attività di Security Awareness verso i dipendenti (12), il Governo della sicurezza (12) e le Attività di Security Awareness verso la clientela (11).

Le Funzioni di Incident Response rappresentano l'ambito maggiormente caratterizzato da una distribuzione tra settori IT e non IT (7), mentre le Attività di testing di Red Teaming, le Funzioni di Digital forensics e le Funzioni di Cyber Threat Intelligence risultano le più frequentemente esternalizzate (6) (Figura 9).

Box 2 – Principali normative europee sulla cyber security

Negli ultimi anni l'Unione europea ha progressivamente rafforzato il quadro normativo in materia di sicurezza informatica e resilienza operativa digitale, con l'obiettivo di accrescere la capacità delle organizzazioni di prevenire, resistere e reagire agli attacchi informatici e agli eventi in grado di compromettere la continuità dei servizi essenziali.
*Per il settore finanziario assume particolare rilievo il Regolamento UE/2022/2554 (**Digital Operational Resilience Act, DORA**) relativo alla resilienza operativa digitale, applicabile dal 17 gennaio 2025. Il Regolamento introduce un quadro unitario per la gestione del rischio ICT, la segnalazione degli incidenti informatici, la gestione del rischio derivante dai fornitori terzi di servizi ICT e la condivisione delle informazioni sulle minacce informatiche. DORA rappresenta il principale riferimento normativo europeo per la resilienza operativa digitale delle entità finanziarie.*
*Accanto a DORA si colloca la Direttiva UE/2022/2555 (**Network and Information Security Directive, NIS2**), che amplia il campo di applicazione della precedente Direttiva NIS e rafforza i requisiti in materia di gestione dei rischi cyber, sicurezza della catena di fornitura, gestione degli incidenti, continuità operativa e responsabilità degli organi di amministrazione. La direttiva costituisce il quadro generale europeo per la cyber security delle infrastrutture e dei servizi essenziali e importanti.*
*In tale contesto si inserisce anche la Direttiva UE/2022/2557 (**Critical Entities Resilience, CER**) sulla resilienza dei soggetti critici, finalizzata a rafforzare la capacità delle organizzazioni operanti in settori strategici di far fronte, in termini di prevenzione e reazione, a eventi in grado di compromettere l'erogazione di servizi essenziali, comprese le minacce ibride e cyber.*
*Completa il quadro il Regolamento UE/2024/2847 (**Cyber Resilience Act, CRA**), che introduce requisiti orizzontali di cyber security per i prodotti con elementi digitali, prevedendo obblighi relativi alla sicurezza lungo l'intero ciclo di vita del prodotto, alla gestione delle vulnerabilità e agli aggiornamenti di sicurezza.*

Fonti

Regolamento UE/2022/2554 (Digital Operational Resilience Act, DORA)
https://eur-lex.europa.eu/eli/reg/2022/2554/oj
Direttiva UE/2022/2555 (Network and Information Security Directive 2, NIS2)
https://eur-lex.europa.eu/eli/dir/2022/2555/oj
Direttiva UE/2022/2557 (Critical Entities Resilience, CER)
https://eur-lex.europa.eu/eli/dir/2022/2557/oj
Regolamento UE/2024/2847 (Cyber Resilience Act, CRA)
https://eur-lex.europa.eu/eli/reg/2024/2847/oj

Capitolo 2. Aspetti economici e organizzativi

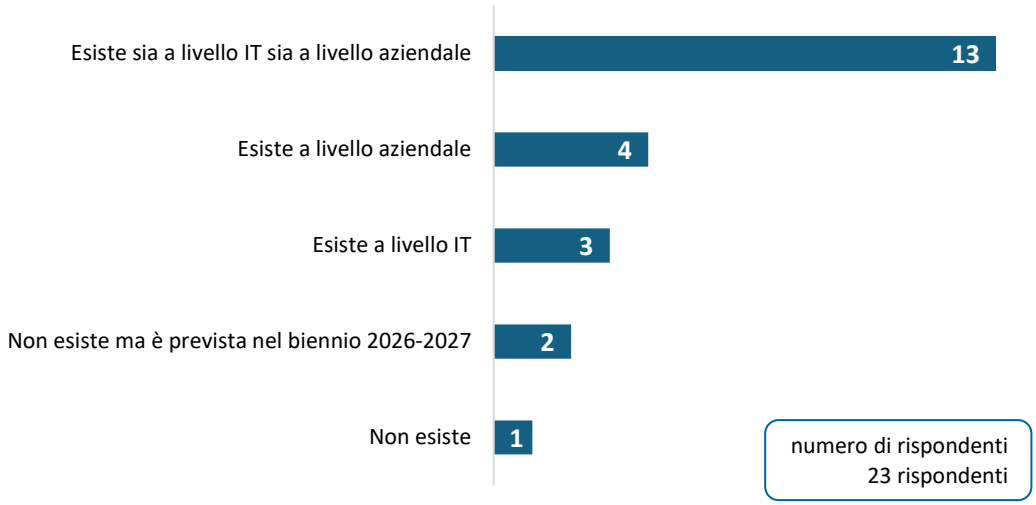
Il secondo capitolo esamina gli aspetti economici e organizzativi della sicurezza informatica nel settore bancario. L'analisi approfondisce le metodologie adottate per la rilevazione dei costi e degli investimenti destinati alla sicurezza, le competenze specialistiche disponibili e i relativi gap rispetto ai fabbisogni in prospettiva, i modelli organizzativi adottati per la gestione delle funzioni di sicurezza, nonché i requisiti professionali richiesti, le modalità di reperimento delle competenze e le iniziative di formazione, con particolare riferimento agli ambiti della cyber security.

2.1 Costi e investimenti per la sicurezza informatica

In questo paragrafo vengono esaminati gli aspetti economici della sicurezza informatica, con particolare riferimento alle metodologie adottate per la rilevazione dei costi, nonché alle caratteristiche del budget IT dedicato alla sicurezza informatica.

Domanda: *Indicare se la banca/gruppo si avvale di una metodologia per la rilevazione dei costi legati alla sicurezza informatica.*

Figura 10 – Metodologia per la rilevazione dei costi

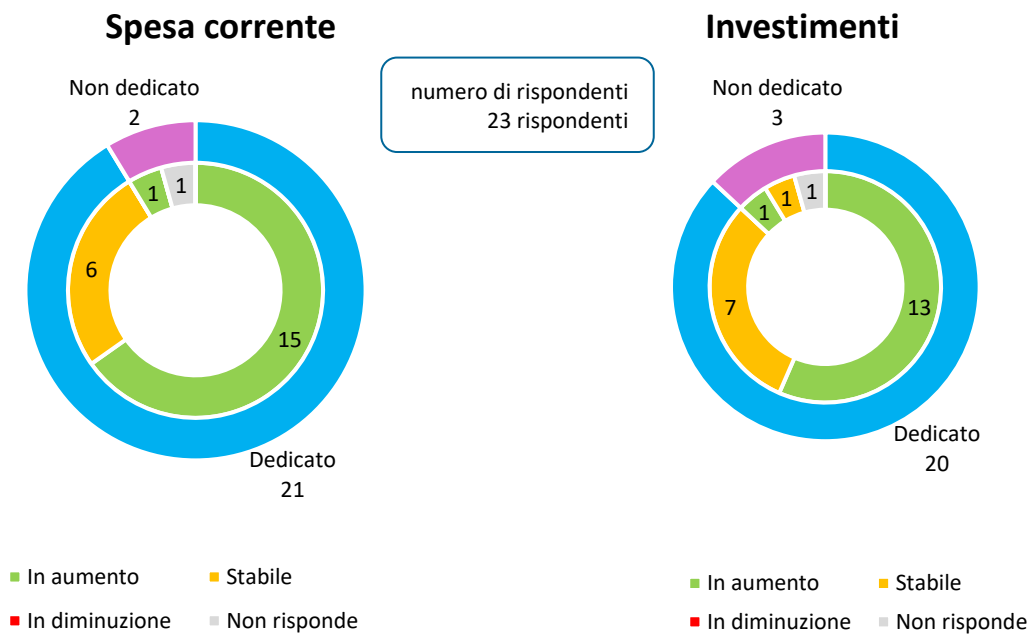


La maggior parte dei rispondenti dichiara di avvalersi di una metodologia per la rilevazione dei costi destinati alla sicurezza: 13 banche adottano una metodologia sia a livello IT sia a livello aziendale, quattro dispongono di metodologie a livello aziendale e tre a livello IT.

Risulta contenuto il numero delle banche che non si sono ancora dotate di una metodologia dedicata: due ne prevedono l'introduzione nel biennio 2026-2027 e una sola banca dichiara di non prevederne l'introduzione in prospettiva (Figura 10).

Domanda: *Con riferimento al Budget IT 2026, specificare se per la sicurezza informatica è previsto uno stanziamento dedicato e indicare il trend rispetto all'anno precedente, distinguendo tra investimenti e spesa corrente.*

Figura 11 – Budget IT 2026 - tipologia di stanziamento



Nel complesso, i risultati confermano il crescente impegno economico destinato al rafforzamento della sicurezza informatica. Per il 2026 quasi tutti i rispondenti prevedono un budget IT dedicato alla sicurezza informatica, sia in termini di spesa corrente sia di investimenti. In particolare, 21 banche dichiarano uno stanziamento dedicato per la spesa corrente e 20 per gli investimenti. L'andamento della spesa corrente e degli investimenti, per 15 e 13 banche rispettivamente, risulta in aumento rispetto all'anno precedente. Per un terzo circa risulta stabile (Figura 11).

2.2 Competenze attuali e richieste

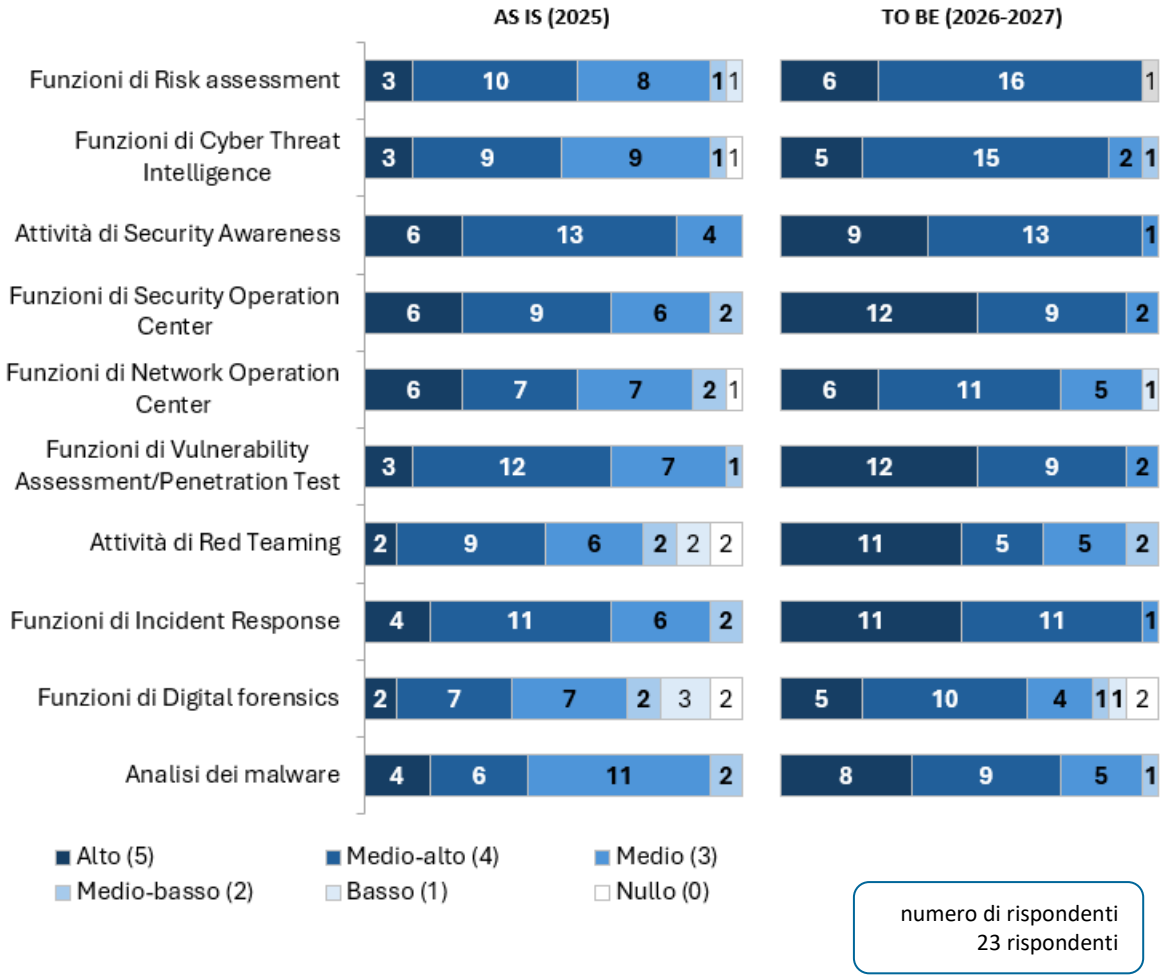
Le competenze rappresentano un elemento chiave per l'efficacia dei processi di sicurezza informatica. Sebbene ciascun ambito della sicurezza richieda conoscenze specialistiche e professionalità dedicate, assume un'importanza crescente la diffusione di una cultura della sicurezza e di una maggiore consapevolezza dei rischi cyber all'interno dell'intera organizzazione.

La stretta collaborazione tra figure specialistiche e funzioni operative e di business contribuisce a integrare la sicurezza nei processi aziendali e a rafforzare la capacità complessiva dell'organizzazione di prevenire, individuare e gestire le minacce informatiche.

Nei paragrafi che seguono, l'analisi si concentra in particolare sulle competenze specialistiche riguardanti le principali funzioni di sicurezza informatica, esaminandone il livello di copertura attuale, le esigenze di rafforzamento previste nel biennio 2026-2027 e le modalità di reperimento degli skill.

Domanda: *Con riferimento alle attività elencate nel seguito, indicare il livello di copertura delle competenze presenti nella banca/gruppo (AS IS), quello da raggiungere nel biennio 2026-2027 (TO BE) e la modalità prevalente di reperimento delle competenze IT.*

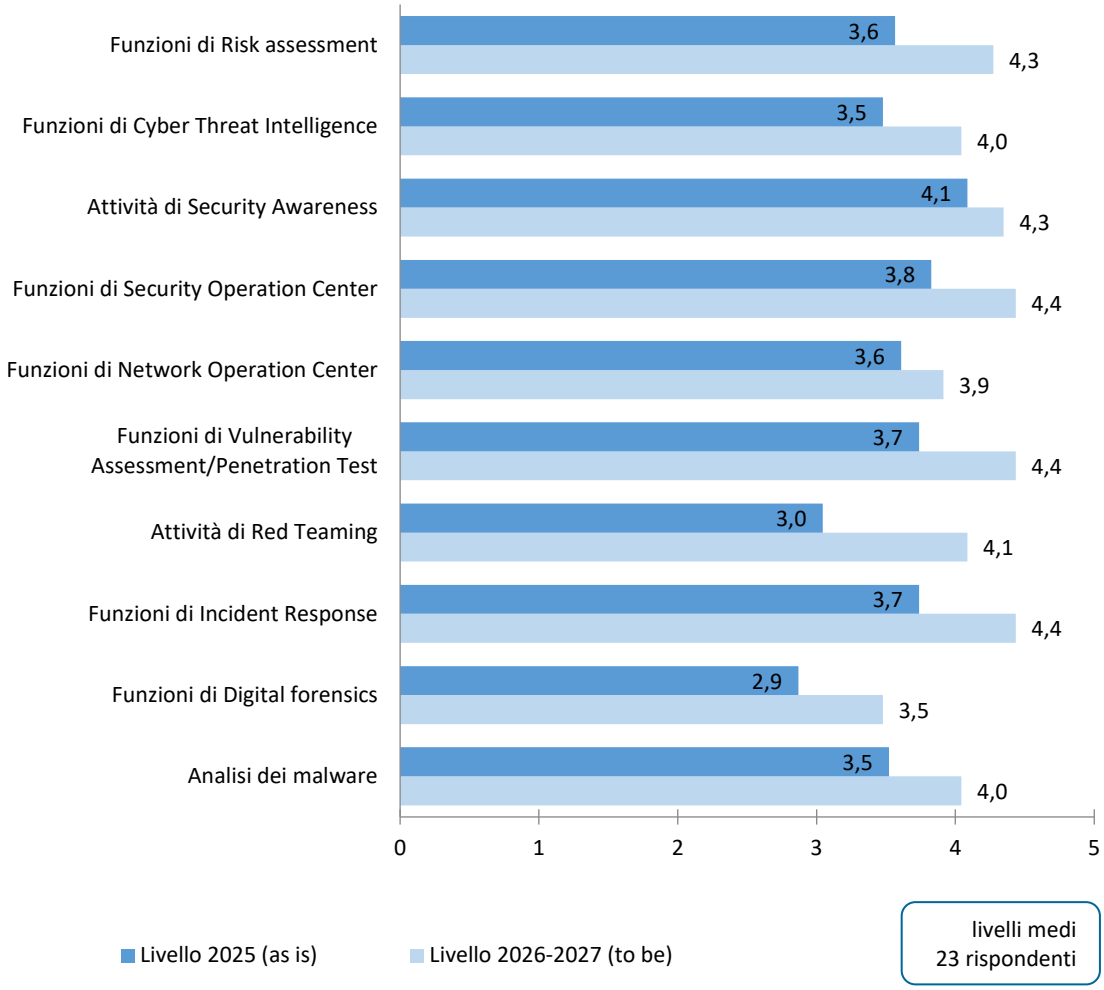
Figura 12 – Competenze IT: AS IS e TO BE



La distribuzione dei livelli di competenza riportata nella Figura 12 evidenzia come i rispondenti collochino prevalentemente le proprie competenze attuali nei livelli medi e medio-alti[3] della scala proposta, mentre per il biennio 2026-2027 emerge uno spostamento verso livelli più elevati. Per una lettura sintetica e comparativa dei risultati si rimanda alla figura che segue, che ne fornisce una rappresentazione aggregata.

[3] Presentano infatti un valore superiore a 3 in una scala proposta da 0 a 5.

Figura 13 – Competenze: AS IS e TO BE

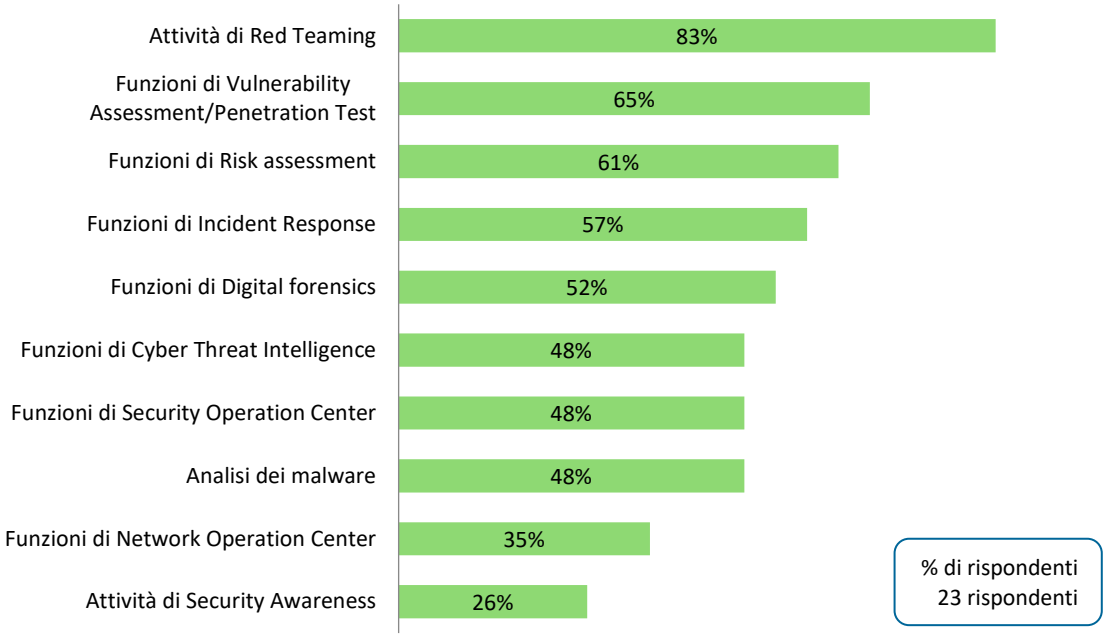


La Figura 13 mostra che le banche ritengono di possedere, già al 2025, competenze specialistiche nell'ambito della sicurezza informatica ad un livello di copertura medio-alto[3]. I valori più alti si riscontrano nelle Attività di Security Awareness (4.1), nelle Funzioni di Security Operation Center (3.8), nelle Funzioni di Vulnerability Assessment/Penetration Test (3.7), mentre valori inferiori caratterizzano le Attività di Red Teaming (3.0) e le Funzioni di Digital forensics (2.9).

Per il biennio 2026-2027 le banche prevedono un rafforzamento delle competenze in tutti gli ambiti considerati. La differenza tra il livello di copertura attuale delle competenze e quello ritenuto necessario nel biennio 2026-2027 consente di individuare i principali gap percepiti dai rispondenti nelle diverse funzioni di sicurezza.

Gli incrementi più significativi (gap) riguardano le Attività di Red Teaming (1.1), le attività di Risk assessment, le Funzioni di Vulnerability Assessment/Penetration Test (0.7), le Funzioni di Incident Response (0.7) e le Funzioni di Security Operation Center (0.6), a conferma della crescente attenzione verso le attività di prevenzione, rilevazione e risposta alle minacce informatiche.

Figura 14 – GAP di competenze

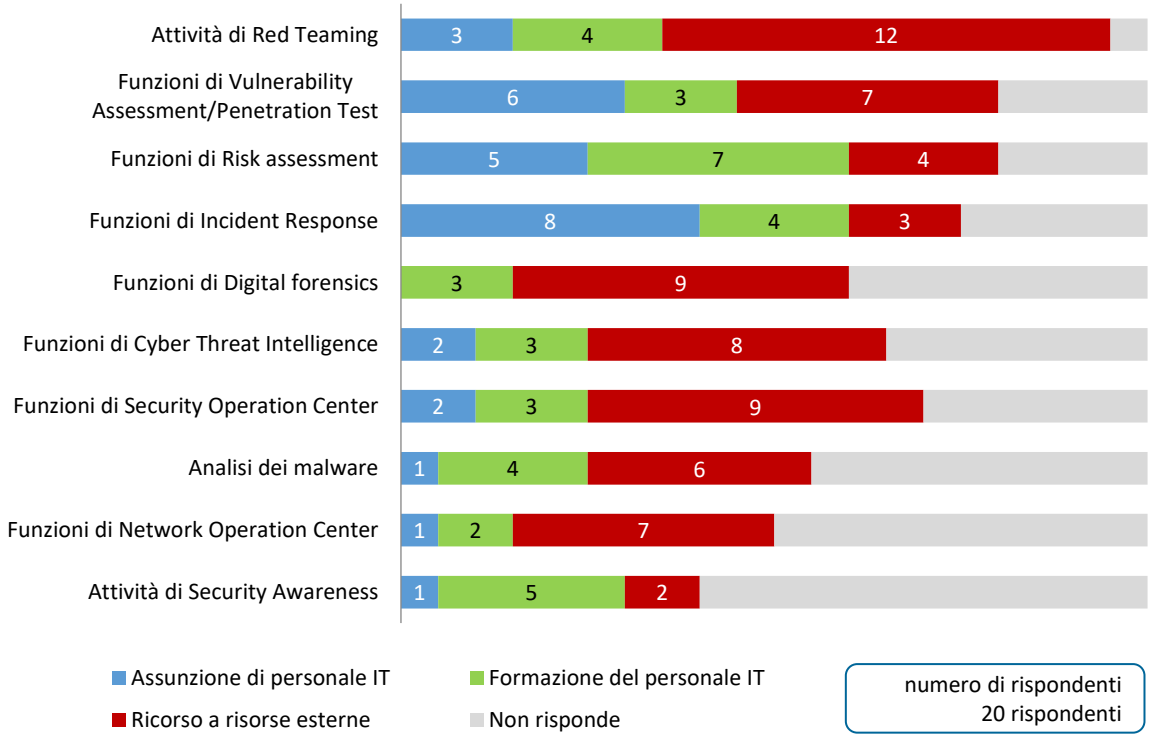


Nella Figura 14 è rappresentata la percentuale di banche che ha indicato un gap di competenza tra il livello attuale e quello previsto per il biennio 2026-2027 in considerazione della specifica funzione di sicurezza.

Si conferma che le segnalazioni ricorrono in prevalenza nelle Attività di Red Teaming (83%), nelle Funzioni di Vulnerability Assessment/Penetration Test (65%) e nelle Funzioni di Risk assessment (61%). Seguono le Funzioni di Incident Response (57%), le Funzioni di Digital forensics (52%).

In misura inferiore emergono segnalazioni nelle Attività di Security Awareness (26%).

Figura 15 – Modalità di reperimento competenze



Nel complesso i risultati evidenziano come le banche tendano a privilegiare il ricorso a risorse esterne negli ambiti caratterizzati da maggiore specializzazione tecnica e innovazione, mentre per le attività che richiedono una competenza più trasversale e integrata, si registra un maggior ricorso all'assunzione di personale e alla formazione del personale IT.

Infatti, il ricorso a risorse esterne rappresenta la modalità prevalente di reperimento delle competenze per le Attività di Red Teaming (12 rispondenti) e risulta particolarmente frequente nelle Funzioni di Digital forensics (9), nelle Funzioni di Security Operation Center (9), nelle Funzioni di Cyber Threat Intelligence (8).

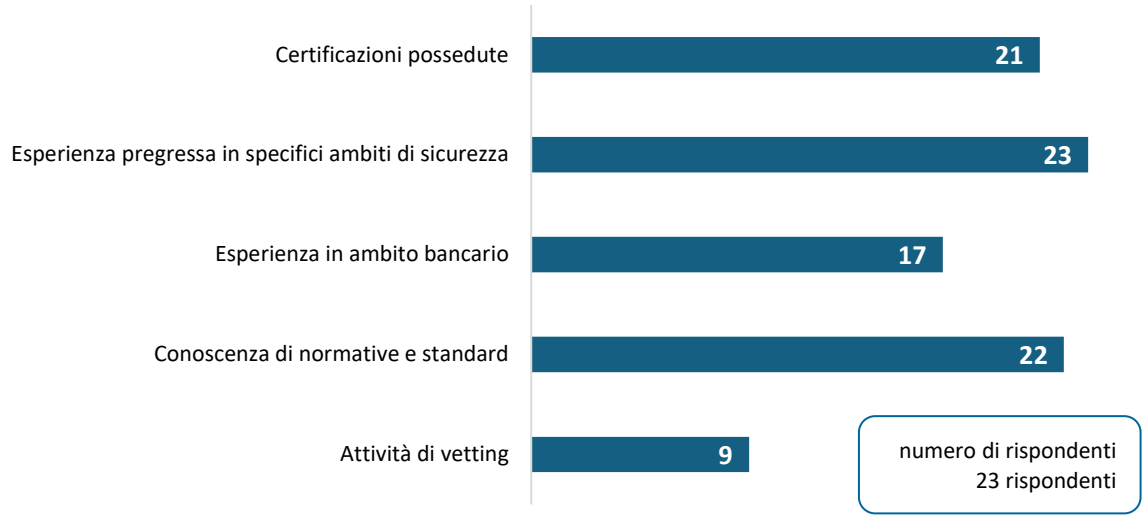
L'assunzione di personale IT è maggiormente utilizzata nelle Funzioni di Incident Response (8) e nelle Funzioni di Vulnerability Assessment/Penetration Test (6), e la formazione del personale IT assume il ruolo più rilevante nelle Funzioni di Risk assessment IT (7) e nelle Attività di Security Awareness (5) (Figura 15).

2.3 Assunzione, formazione e requisiti

L'analisi prosegue esaminando i requisiti richiesti per l'assunzione del personale specializzato in sicurezza informatica, i principali istituti e le certificazioni professionali di riferimento, le iniziative di formazione adottate dai rispondenti per il rafforzamento e l'aggiornamento delle competenze, anche negli ambiti della cyber security.

Domanda: *Con riferimento all'assunzione di personale, indicare quali requisiti vengono considerati nella valutazione di un candidato esperto in sicurezza informatica.*

Figura 16 – Requisiti per l'assunzione di esperti in sicurezza informatica



Tra i requisiti considerati nella valutazione di un candidato esperto in sicurezza informatica assume particolare rilevanza l'Esperienza pregressa in specifici ambiti di sicurezza, indicata da tutti i rispondenti (23). Le certificazioni professionali possedute sono considerate da 21 rispondenti.

I risultati evidenziano inoltre come, accanto alle competenze tecniche specialistiche, assumano importanza anche conoscenze e competenze trasversali, quali la Conoscenza di normative e standard (22) e l'Esperienza in ambito bancario (17). Sono considerate per nove rispondenti le Attività di vetting, vale a dire l'insieme delle verifiche preventive effettuate dall'organizzazione sulla persona prima dell'assunzione o dell'assegnazione a ruoli che comportano l'accesso a informazioni, sistemi o infrastrutture sensibili (Figura 16).

Domanda: *Con riferimento alla formazione e all'assunzione del personale tecnico specializzato in sicurezza informatica, indicare, tra i seguenti istituti di formazione, quelli a cui la banca/gruppo ricorre prevalentemente. Specificare inoltre le prime tre certificazioni di riferimento.*

Figura 17 – Ricorso a istituti di formazione

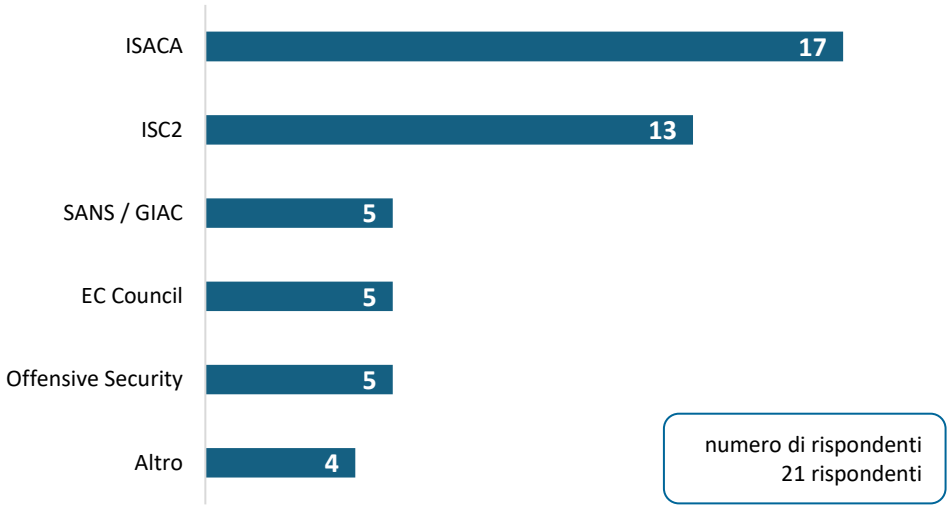
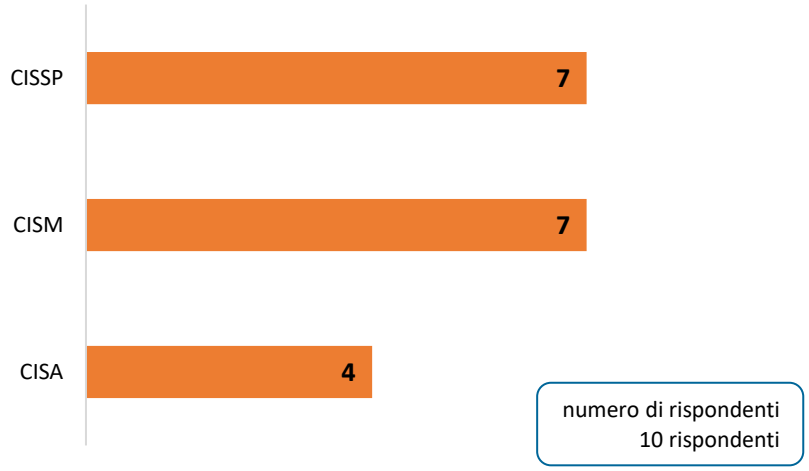


Figura 18 – Certificazioni professionali di riferimento



Tra gli istituti e gli organismi di riferimento per la formazione e la certificazione professionale del personale esperto di sicurezza informatica, i rispondenti indicano prevalentemente ISACA (17) e ISC2 (13). Si tratta di istituti che erogano percorsi trasversali, orientati alla governance, alla gestione del rischio e alla conformità normativa di tipo internazionale.

D'altra parte, emerge anche il ricorso a istituti di formazione che erogano iniziative formative a elevato contenuto tecnico-specialistico nell'ambito dell'analisi delle minacce, dei test e delle attività di sicurezza offensiva, caratterizzati da una continua evoluzione delle tecniche e dei relativi strumenti di contrasto quali SANS/GIAC (5), EC Council (5) e Offensive Security (5) (Figura 17).

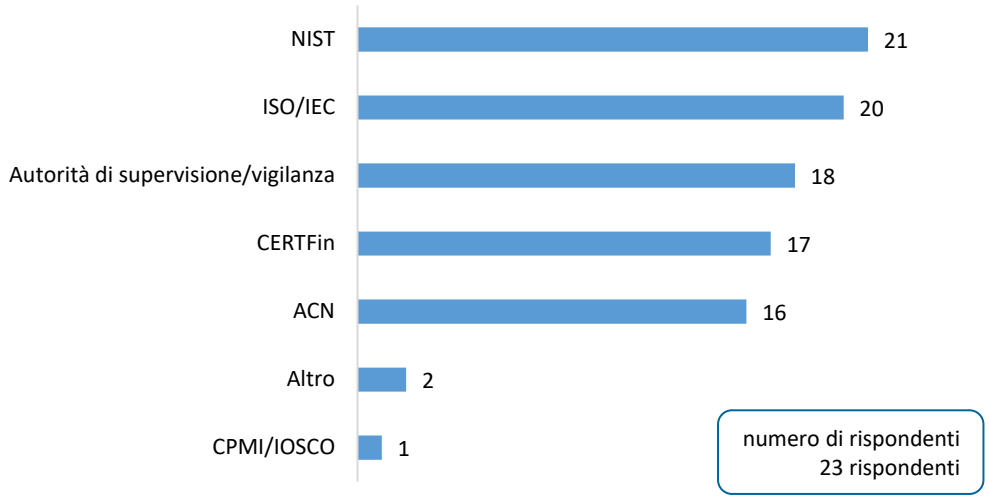
Riguardo le tre certificazioni professionali di riferimento indicate dai rispondenti, nella Figura 18 emergono la Certified Information Systems Security Professional - CISSP e la Certified Information Security Manager - CISM (7). Segue la Certified Information Systems Auditor - CISA (4).

I risultati evidenziano una prevalenza di certificazioni orientate alla governance della sicurezza e alla gestione del rischio, a conferma della crescente attenzione del settore bancario verso competenze in grado di coniugare aspetti tecnologici, organizzativi e normativi.

La presenza della certificazione CISA, tra le principali di riferimento, evidenzia l'attenzione verso le attività di audit, controllo e verifica dell'efficacia dei presidi di sicurezza.

Domanda: *Con riferimento a standard, linee guida e framework in materia di sicurezza informatica, indicare quali organismi vengono maggiormente considerati dalla banca/gruppo (Risposta multipla).*

Figura 19 – Organismi di riferimento considerati



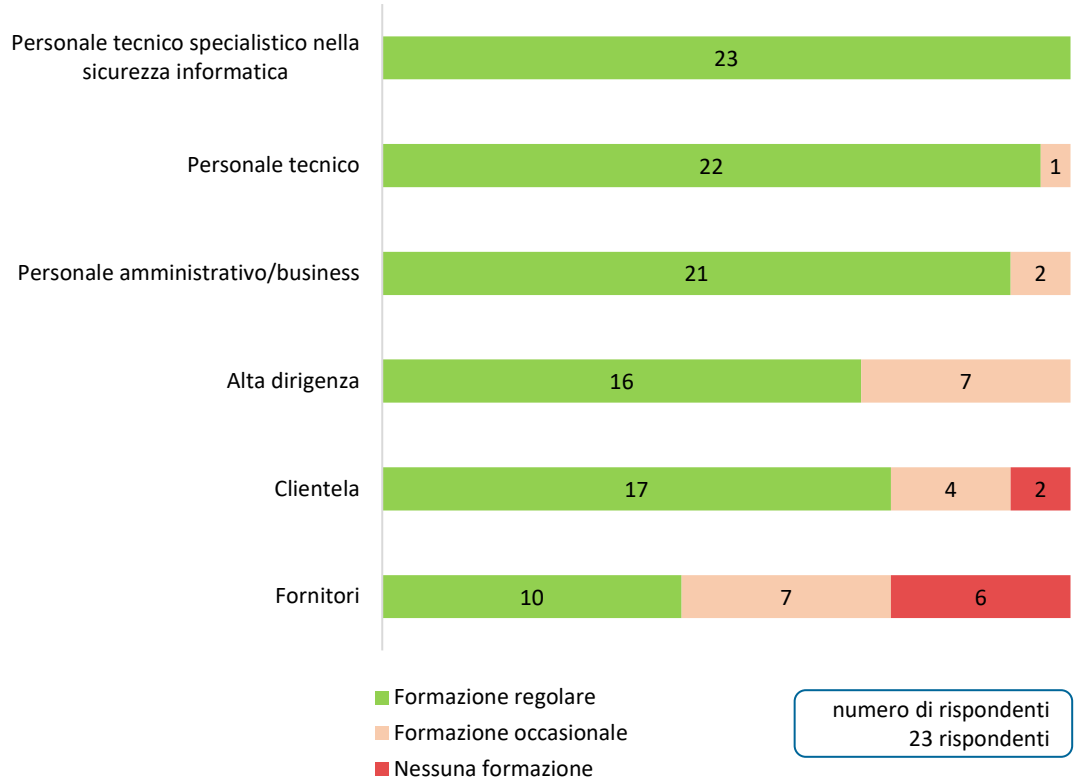
I risultati (Figura 19) evidenziano come le banche facciano riferimento a un insieme articolato di standard, framework, linee guida e indirizzi operativi provenienti sia dal contesto internazionale sia da quello nazionale. Accanto ai framework metodologici e agli standard di riferimento, assumono particolare rilevanza le indicazioni provenienti dalle autorità di vigilanza e dagli organismi specializzati nella condivisione e nell'analisi delle minacce informatiche.

Per i rispondenti, i principali organismi di riferimento in materia di sicurezza informatica sono il NIST (21) e l'ISO/IEC (20), seguiti dalle Autorità di supervisione e vigilanza (18), dal CERTFin (17) e dall'Agenzia per la Cybersicurezza Nazionale - ACN (16).

Domanda: *Con riferimento al processo "9. Formazione e Awareness di sicurezza"[4], indicare se la banca/gruppo svolge iniziative formative in tema di sicurezza informatica, per i destinatari di seguito elencati, e specificarne la periodicità.*

[4] Cfr. Figura 6

Figura 20 – Destinatari della formazione in sicurezza informatica



Le iniziative di formazione in materia di sicurezza informatica risultano ampiamente diffuse tra i rispondenti. In particolare, tutti dichiarano di svolgere attività regolare di formazione nei confronti del Personale tecnico specialistico nella sicurezza informatica (23) e quasi tutti al Personale tecnico (22) e al Personale amministrativo/business (21).

Per una consistente quota di rispondenti la formazione regolare si indirizza anche alla Clientela (17) e all'Alta dirigenza (16). Per queste categorie emerge anche una presenza di iniziative svolte con carattere occasionale, rispettivamente per 4 e 7 rispondenti.

Le iniziative formative rivolte ai Fornitori risultano meno frequenti e interessano complessivamente 17 rispondenti, dei quali 10 dichiarano attività di formazione regolare e 7 occasionale (Figura 20).

Capitolo 3. Contesto geopolitico e focus su processi di sicurezza

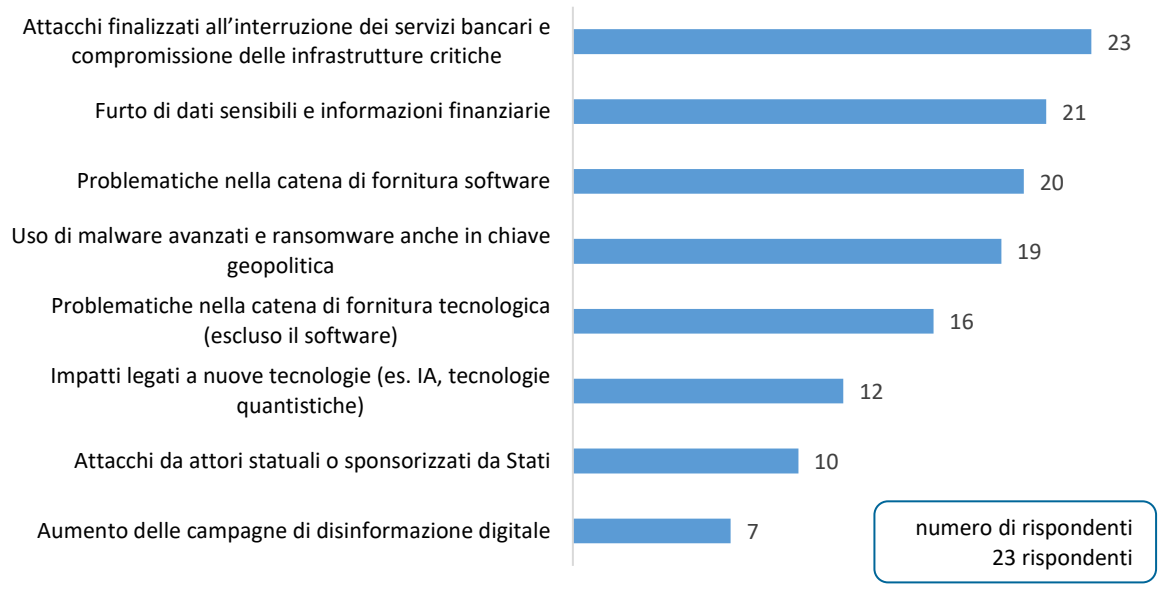
Il presente capitolo, a partire dall'esame delle minacce del contesto geopolitico, approfondisce alcuni processi di sicurezza rilevanti alla luce dell'evoluzione della minaccia cyber. In particolare, l'analisi prende avvio dal processo di Risk assessment IT, per poi analizzare un sottoinsieme di ulteriori processi di sicurezza significativi con l'obiettivo di evidenziarne caratteristiche e livello di maturità presso le banche. Completa il quadro l'esame sull'utilizzo di tecnologie innovative nell'ambito della sicurezza, quali l'Intelligenza Artificiale e il Quantum Computing, nonché ulteriori approfondimenti relativi al cloud, a piattaforme di base utili anche nell'ambito della sicurezza e alle modalità di autenticazione.

3.1 Minacce cyber e contesto geopolitico

In questo paragrafo vengono esaminate, alla luce del contesto geopolitico, le principali minacce nel settore bancario nell'ambito del processo di valutazione del rischio e il grado di integrazione di tali rischi nei processi di sicurezza già esaminati nel capitolo 1 (cfr. Figura 6).

Domanda: *Con riferimento al processo "4. Risk Assessment IT"[4], indicare quali delle seguenti minacce, che caratterizzano anche il rischio cyber in chiave geopolitica, sono esplicitamente considerate (Risposta multipla).*

Figura 21 – Minacce cyber considerate nel Risk assessment IT



Nel complesso, i risultati della Figura 21 evidenziano come i processi di Risk assessment IT siano principalmente orientati alle minacce in grado di produrre impatti diretti sulla disponibilità dei servizi e sulla riservatezza delle informazioni.

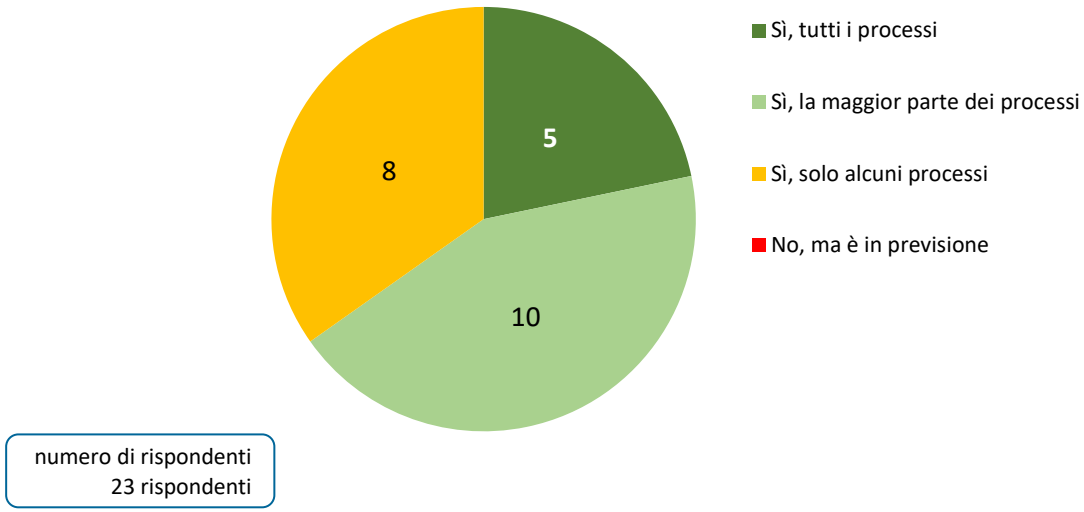
In particolare, nel processo di Risk assessment IT, con riferimento alle minacce cyber, tutti i rispondenti prendono in esame gli Attacchi finalizzati all'interruzione dei servizi bancari e alla compromissione delle infrastrutture critiche (23); seguono il Furto di dati sensibili e informazioni finanziarie (21) e le Problematiche nella catena di fornitura software (20).

Sono segnalati inoltre l'Uso di malware avanzati e ransomware anche in chiave geopolitica (19) e le Problematiche nella catena di fornitura tecnologica - escluso il software (16), a conferma dell'attenzione riservata ai rischi derivanti dalla crescente interconnessione dei sistemi.

Gli Impatti legati a nuove tecnologie, quali l'Intelligenza Artificiale e le tecnologie quantistiche (12) sono segnalati da oltre la metà del campione.

Domanda: *Indicare se i processi di sicurezza tengono esplicitamente conto dei rischi connessi all'attuale contesto geopolitico.*

Figura 22 – Processi di sicurezza e rischi del contesto geopolitico



I risultati della Figura 22 evidenziano che i rischi connessi all'attuale contesto geopolitico sono tenuti in conto da tutti i rispondenti in più di un processo. In particolare, 10 rispondenti li considerano nella maggior parte dei processi di sicurezza, mentre otto li prendono in considerazione solo in alcuni processi.

Un numero più contenuto di rispondenti (5) afferma che i rischi derivanti dal contesto geopolitico sono esplicitamente inclusi in tutti i processi di sicurezza.

3.2 Focus sui processi di sicurezza

In questo paragrafo sono approfonditi alcuni processi di sicurezza ritenuti particolarmente significativi per il settore bancario al fine di evidenziarne modalità di adozione e caratteristiche. In particolare, l'analisi riguarda i processi di Cyber Threat Intelligence, Information Sharing, Security

Assessment - Red Teaming, Vulnerability Assessment e Patch Management, Digital forensics e Gestione del rischio delle terze parti.

Nota metodologica 1: *Per i grafici (dalla figura 23 alla figura 29), la legenda, a destra, è stata costruita secondo una logica progressiva di maturità, disponendo in alto e in verde l'opzione associata al livello di maturità più elevato. Le opzioni che seguono in legenda via via sottostanti rappresentano, in generale, livelli di maturità progressivamente inferiori.*

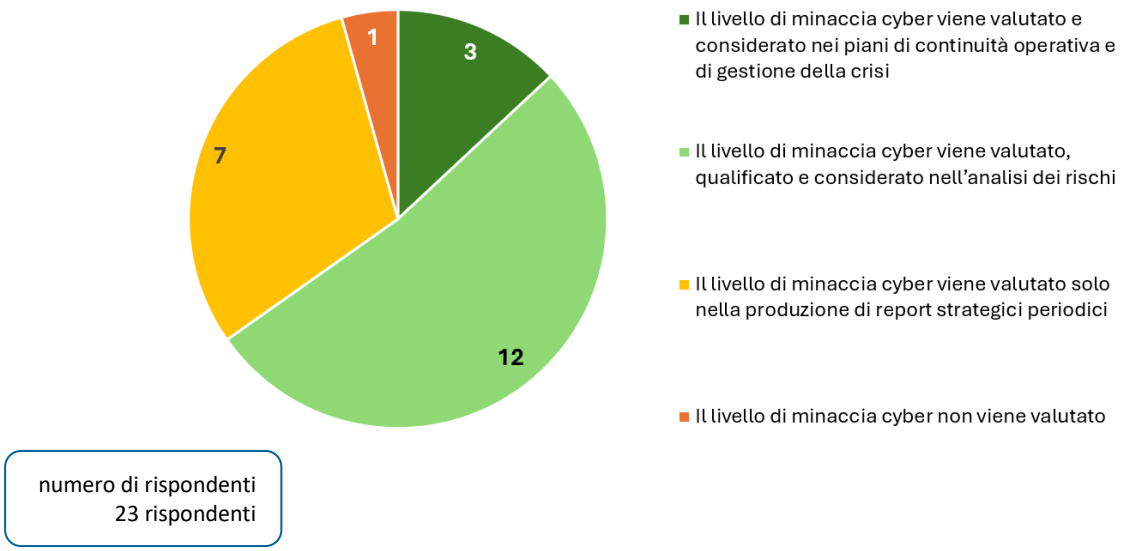
3.3 Cyber Threat Intelligence

La Cyber Threat Intelligence (CTI) rappresenta uno dei processi più rilevanti e innovativi nell'attuale contesto della sicurezza informatica, in quanto consente di raccogliere, analizzare e interpretare informazioni sulle minacce cyber, supportando decisioni strategiche, tattiche e operative dell'organizzazione. L'evoluzione delle tecniche di attacco e la crescente complessità del panorama delle minacce richiedono infatti capacità sempre più avanzate di anticipazione, monitoraggio e adattamento dei presidi di difesa.

In tale contesto, l'indagine ha approfondito sia gli aspetti di tipo strategico legati alla valutazione della minaccia cyber, sia quelli di tipologia più tattico-operativa con l'applicazione di specifiche contromisure.

Domanda: *Con riferimento al processo "3. Cyber Threat Intelligence"[4], indicare se viene valutato, e con quale modalità, il livello della minaccia cyber (Risposta multipla).*

Figura 23 – Cyber Threat Intelligence – Valutazione strategica



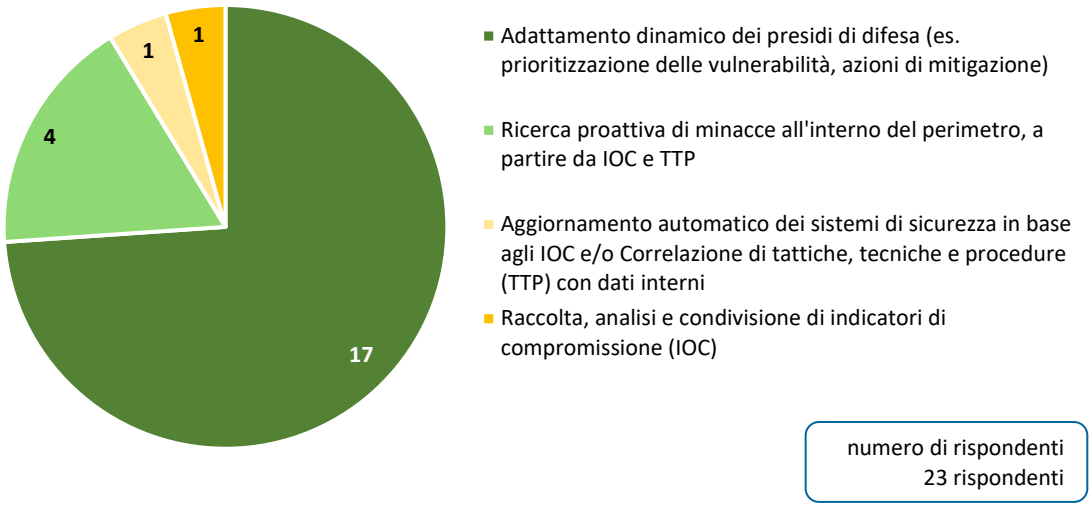
La valutazione strategica della minaccia cyber risulta ampiamente diffusa (22 rispondenti) considerando le prime tre opzioni di risposta della legenda. In particolare, oltre la metà del campione dichiara che il livello della minaccia cyber viene valutato, qualificato e considerato nell'analisi dei rischi (12). Una quota significativa di rispondenti utilizza tali valutazioni in maniera informativa per la produzione di report strategici periodici (7), mentre un numero più contenuto ne

tiene conto anche nell'ambito dei piani di continuità operativa e di gestione della crisi (3), massimo livello di maturità del processo per il supporto alle attività di tipo strategico.

Soltanto un rispondente dichiara che il livello della minaccia cyber non viene valutato (Figura 23).

Domanda: *Con riferimento al processo "3. Cyber Threat Intelligence"[4], qualora presente, indicare quali dei seguenti sotto-processi viene messo in atto per rispondere a livello tattico-operativo alla minaccia cyber (Risposta multipla).*

Figura 24 – Cyber Threat Intelligence – Valutazione tattico-operativa



Nota metodologica 2: *Si precisa che, per la Figura 24, oltre alla logica progressiva di maturità per le opzioni (cfr. Nota metodologica 1), ciascuna opzione del livello di maturità comprende le attività previste dalle opzioni inferiori e sottostanti; pertanto, la selezione di una specifica opzione da parte di un rispondente implica anche l'adozione delle pratiche descritte nelle opzioni che seguono.*

Dall'analisi della Figura 24, la maggior parte dei rispondenti si colloca nella risposta Adattamento dinamico dei presidi di difesa (17), attraverso attività quali la prioritizzazione delle vulnerabilità e l'attuazione di misure di mitigazione in funzione dell'evoluzione della minaccia.

Meno ricorrente è la Ricerca proattiva di minacce all'interno del perimetro aziendale, a partire da indicatori di compromissione (IOC) e tattiche, tecniche e procedure (TTP) individuate (4).

Solo un rispondente dichiara l'Aggiornamento automatico dei sistemi di sicurezza sulla base degli IOC e della correlazione delle TTP con dati interni, così come uno solo seleziona la risposta con il livello di maturità più basso, effettuando esclusivamente la Raccolta, analisi e condivisione di indicatori di compromissione (IOC).

Nel complesso, i risultati delle Figure 23 e 24 evidenziano come la Cyber Threat Intelligence abbia raggiunto, nel 2025, un livello di maturità più elevato nelle attività di tipo tattico-operativo, orientate all'adattamento dei presidi di difesa e delle misure di mitigazione, mentre si evidenziano margini di miglioramento nell'utilizzo della CTI a supporto dei processi decisionali strategici.

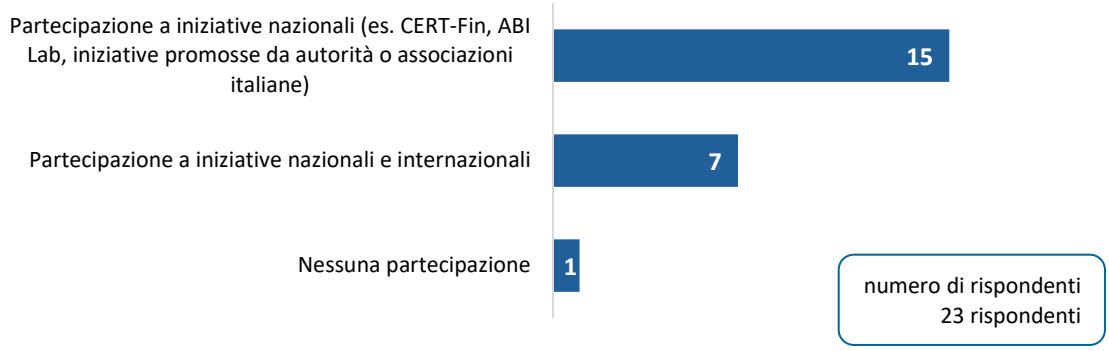
3.4 Processo di Information Sharing

L'Information Sharing è un processo di supporto alle attività di prevenzione, individuazione e gestione delle minacce informatiche, consentendo lo scambio di informazioni, indicatori di compromissione ed elementi di intelligence tra organizzazioni appartenenti a comunità "trusted".

In tale contesto, l'indagine ha approfondito il livello di partecipazione dei rispondenti a iniziative di Information Sharing.

Domanda: *Con riferimento al processo "10. Information Sharing"[4], indicare se la banca/gruppo bancario partecipa a una "trusted community" per lo scambio di informazioni su minacce informatiche, specificando la tipologia di iniziativa.*

Figura 25 – Information Sharing – Partecipazione a iniziative



La partecipazione a iniziative di Information Sharing risulta ampiamente diffusa tra i rispondenti (22). In particolare, la maggior parte dichiara di aderire a iniziative nazionali (15), quali CERT-Fin, ABI Lab e altre iniziative promosse da autorità o associazioni di settore.

Una quota significativa di rispondenti partecipa sia a iniziative nazionali sia internazionali (7), a conferma dell'interesse verso forme di collaborazione e scambio informativo che si estendono oltre il contesto nazionale.

Solo un rispondente dichiara di non partecipare ad alcuna iniziativa (Figura 25).

Box 3 – Information Sharing

L'Information Sharing rappresenta il processo attraverso il quale organizzazioni appartenenti a una medesima comunità di fiducia condividono informazioni relative a minacce informatiche, vulnerabilità, incidenti di sicurezza e modalità di attacco, con l'obiettivo di rafforzare la capacità collettiva di prevenzione e risposta agli eventi cyber.

La condivisione delle informazioni consente ai partecipanti di acquisire maggiore consapevolezza sull'evoluzione delle minacce, ridurre i tempi di individuazione degli attacchi e adottare misure di mitigazione più tempestive. In particolare, possono essere condivisi:

- *Indicatori di compromissione (IOC - Indicators of Compromise), quali indirizzi IP malevoli, domini sospetti, hash di malware e firme di attacco;*
- *Tattiche, tecniche e procedure (TTP - Tactics, Techniques and Procedures) utilizzate dagli attaccanti;*
- *informazioni relative a vulnerabilità emergenti;*
- *evidenze derivanti dalla gestione di incidenti cyber;*
- *analisi e valutazioni prodotte nell'ambito delle attività di Cyber Threat Intelligence.*

Nel settore finanziario tali attività assumono particolare rilevanza in considerazione dell'elevata interconnessione tra gli operatori e della possibilità che una stessa minaccia interessi simultaneamente più soggetti. Per questo motivo, negli ultimi anni si sono diffuse numerose iniziative di collaborazione e scambio informativo a livello nazionale e internazionale.

Anche il quadro normativo europeo riconosce l'importanza dello scambio di informazioni in materia di cyber security. Il Regolamento UE/2022/2554 (Digital Operational Resilience Act, DORA) prevede infatti specifiche disposizioni volte a favorire la partecipazione delle entità finanziarie a meccanismi di condivisione delle informazioni sulle minacce informatiche, nel rispetto delle condizioni di sicurezza e riservatezza previste dalla normativa.

Fonti

Regolamento UE/2022/2554 (Digital Operational Resilience Act, DORA)
https://eur-lex.europa.eu/eli/reg/2022/2554/oj
CERTFin – Computer Emergency Response Team del settore finanziario italiano
https://www.certfin.it
ENISA, Information Sharing and Analysis Practices for Cyber security
https://www.enisa.europa.eu
NIST, Cyber Threat Information Sharing Frameworks
https://www.nist.gov

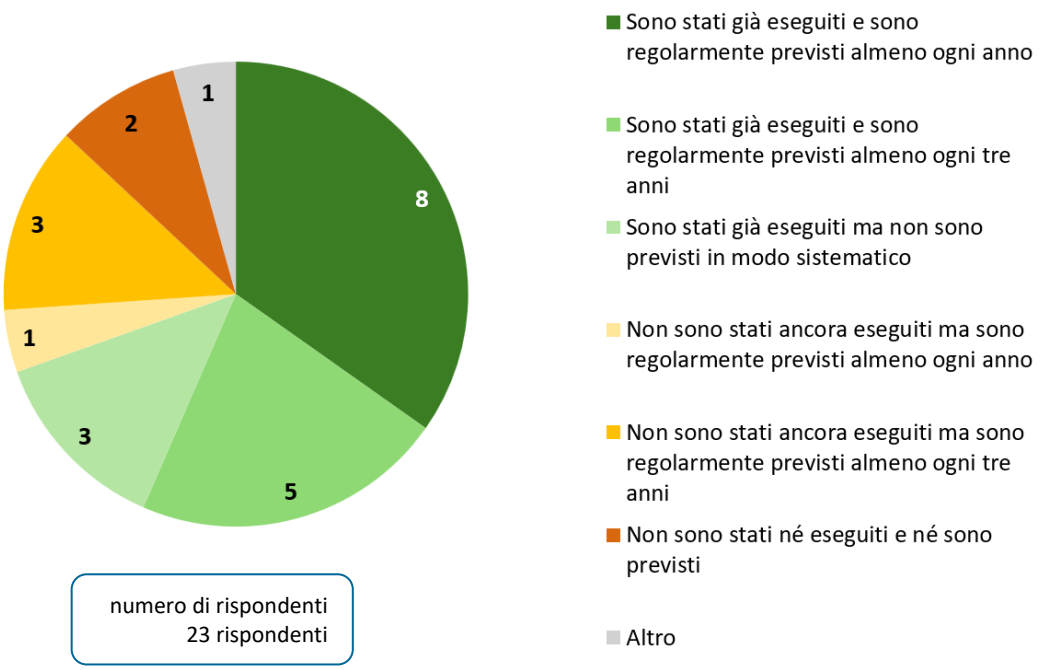
3.5 Processo di Security Assessment – Red Teaming

Le attività di Security Assessment e Testing rivestono un ruolo fondamentale nel verificare l'efficacia dei controlli di sicurezza. Accanto alle tradizionali attività di verifica delle vulnerabilità e di penetration testing, assumono crescente rilevanza gli esercizi di Red Teaming, che consentono di simulare attacchi realistici e mirati, valutando non solo i presidi tecnologici ma anche l'efficacia dei processi organizzativi.

In tale contesto, l'indagine ha approfondito il grado di sistematicità con cui tali esercizi vengono condotti dai rispondenti.

Domanda: *Oltre ai test previsti dalla normativa DORA, indicare se sono stati eseguiti e/o previsti esercizi di tipo Red Teaming (ad es. TLPT e test TIBER-EU/IT).*

Figura 26 – Security Assessment – Red Teaming



Nel complesso, i risultati evidenziano una significativa attenzione verso le attività di Red Teaming. In particolare, dall'analisi emerge, considerando anche la previsione, che essi sono eseguiti o previsti per 21 rispondenti.

Oltre la metà del campione dichiara di aver già eseguito tali esercizi e di prevederne lo svolgimento con cadenza regolare, annuale (8) o almeno triennale (5).

Un ulteriore gruppo di rispondenti ha già effettuato esercizi di Red Teaming ma non ne prevede ancora l'esecuzione secondo una pianificazione sistematica (3), mentre quattro rispondenti, pur non avendoli ancora eseguiti, ne prevedono l'introduzione con frequenza triennale (3) o annuale (1).

Risultano solo due i rispondenti che non hanno né eseguito né pianificato esercizi di Red Teaming (Figura 26).

Box 4 – Red Teaming, TIBER-IT e quadro normativo DORA

I test di tipo Red Teaming rappresentano attività di verifica di sicurezza finalizzate a simulare attacchi realistici e mirati nei confronti di un'organizzazione. A differenza dei tradizionali test di sicurezza, tentano di verificare sia la concreta possibilità di sfruttamento di vulnerabilità dei sistemi ICT sia la capacità complessiva dell'organizzazione di individuare, contenere e gestire un attacco.

I test avanzati di tipo Threat-Led Penetration Testing (TLPT) sono una tipologia di test di Red Teaming che consiste in tentativi controllati di compromettere la resilienza operativa di un'organizzazione emulando le tattiche, le tecniche e le procedure d'attacco avanzate adottate da reali attori della minaccia nei confronti di persone, processi e tecnologie. I TLPT inoltre simulano scenari di minaccia realistici individuati sulla base di attività di Cyber Threat Intelligence e sono pianificati e condotti con un approccio risk-based allo scopo di minimizzarne gli impatti sull'operatività dell'organizzazione.

Il Regolamento UE/2022/2554 (Digital Operational Resilience Act, DORA) prevede l'esecuzione di specifiche attività di Threat Led Penetration Testing (TLPT) per alcune tipologie di entità finanziarie individuate dalle autorità competenti sulla base della loro rilevanza sistemica e del relativo profilo di rischio. Tali attività devono essere condotte secondo requisiti metodologici definiti dalla normativa e dai correlati standard tecnici.

In tale contesto si colloca il framework TIBER-IT (Threat Intelligence-Based Ethical Red Teaming), promosso in Italia da Banca d'Italia, CONSOB e Ivass, che fornisce una metodologia armonizzata per la conduzione di esercizi avanzati basati sulla simulazione di minacce realistiche e sull'utilizzo della Cyber Threat Intelligence.

Le organizzazioni possono svolgere test di Red Teaming o TLPT indipendentemente dagli obblighi normativi, nell'ambito delle attività di miglioramento della propria postura di cyber security e di resilienza operativa.

Fonti

Regolamento UE/2022/2554 – (Digital Operational Resilience Act, DORA)
https://eur-lex.europa.eu/eli/reg/2022/2554/oj
Banca d'Italia – TIBER-IT
https://www.bancaditalia.it/compiti/sispaga-mercati/tiber-it/index.htm

3.6 Vulnerability assessment e Patch management

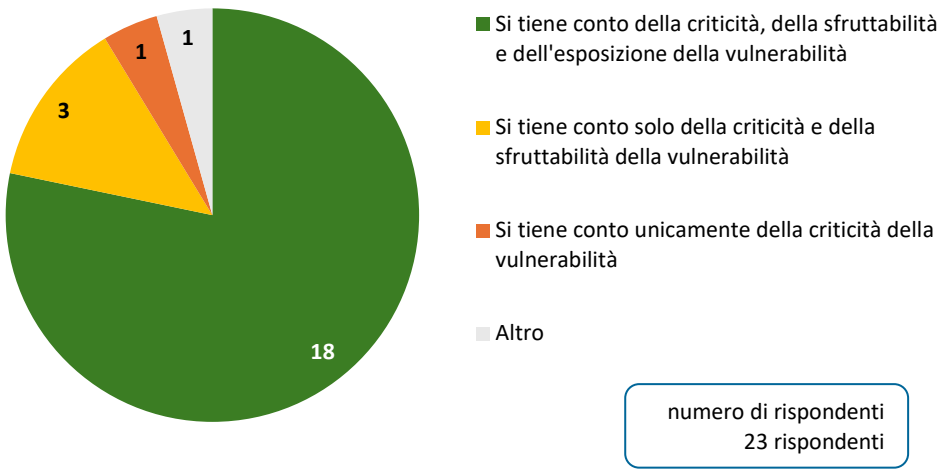
L'attenzione verso il processo di Vulnerability assessment e Patch management assume particolare rilevanza nell'attuale contesto della minaccia cyber, caratterizzato da una crescente capacità degli attaccanti di individuare e sfruttare vulnerabilità mediante strumenti sempre più avanzati, inclusi quelli basati sull'Intelligenza Artificiale.

In tale contesto, un elemento centrale è rappresentato dalla capacità di definire adeguate priorità di intervento. La prioritizzazione delle vulnerabilità costituisce infatti un fattore essenziale per l'efficacia del processo di Patch management. Un approccio orientato alla correzione indiscriminata di tutte le vulnerabilità potrebbe risultare troppo oneroso e non sempre compatibile con le esigenze operative dell'organizzazione; inoltre, le attività di aggiornamento dei sistemi, devono essere governate, per non comportare impatti sulla continuità dei servizi.

In tale contesto, l'indagine ha approfondito i criteri adottati dai rispondenti per la prioritizzazione degli interventi di mitigazione e correzione delle vulnerabilità.

Domanda: *Con riferimento alla Cyber security e al processo "7. Vulnerability e Patch Management"[4], indicare se le vulnerabilità di tipo infrastrutturale e/o applicativo prevedono la valutazione della prioritizzazione degli interventi.*

Figura 27 – Vulnerability Assessment e Patch Management



La maggior parte dei rispondenti dichiara di adottare criteri evoluti di prioritizzazione degli interventi di mitigazione delle vulnerabilità. In particolare, 18 considerano congiuntamente la Criticità, la Sfruttabilità e l'Esposizione della vulnerabilità, adottando quindi un approccio che tiene conto sia delle caratteristiche tecniche della vulnerabilità sia del contesto nel quale essa si manifesta (ad es. Intranet o Internet).

Un numero più contenuto di rispondenti tiene conto della Criticità e della Sfruttabilità della vulnerabilità (3), mentre risultano residuali i casi in cui la prioritizzazione si basa unicamente sulla Criticità della vulnerabilità (1) (Figura 27).

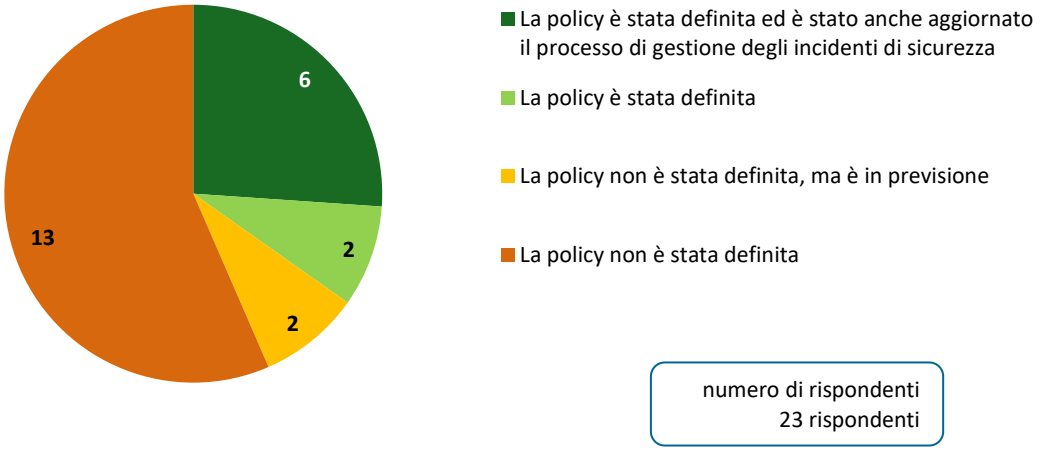
3.7 Processo di Digital forensics

La capacità di raccogliere, conservare e analizzare correttamente le evidenze digitali assume un ruolo sempre più importante nell'ambito della gestione degli incidenti di sicurezza. In un contesto caratterizzato da minacce cyber sempre più sofisticate e dalla crescente rilevanza degli aspetti normativi e probatori, la predisposizione preventiva di procedure e strumenti dedicati consente alle organizzazioni di rafforzare le proprie capacità di risposta agli incidenti e di supportare eventuali attività investigative. La “forensic readiness” rappresenta un elemento di maturità, in quanto consente di predisporre in anticipo procedure, ruoli e strumenti necessari per acquisire e preservare le evidenze digitali, riducendo tempi e complessità delle attività successive a un incidente informatico.

In tale contesto, l'indagine ha approfondito il livello di diffusione delle pratiche di definizione di policy di “forensic readiness” presso i rispondenti.

Domanda: *In relazione al processo “13. Digital forensics”[4], indicare se l’organizzazione ha definito una policy di “forensic readiness”, selezionando una delle opzioni elencate.*

Figura 28 – Definizione policy di Forensic Readiness



I risultati evidenziano un livello di adozione ancora contenuto delle buone prassi di "forensic readiness". In particolare, oltre la metà dei rispondenti dichiara di non aver definito una policy dedicata (13). Su 23 rispondenti solo sei dichiarano infatti di aver definito una policy di forensic readiness e di aver contestualmente aggiornato il processo di gestione degli incidenti di sicurezza, mentre due hanno definito la policy. In previsione ulteriori due rispondenti definiranno la policy (Figura 28).

3.8 Gestione del rischio di terze parti

La gestione del rischio delle terze parti assume un ruolo sempre più rilevante nel contesto della sicurezza informatica del settore bancario, caratterizzato da una crescente dipendenza da fornitori esterni, servizi digitali e infrastrutture condivise. L'ampliamento degli ecosistemi tecnologici e l'interconnessione tra organizzazioni rendono infatti necessario estendere le attività di controllo e monitoraggio anche ai soggetti esterni che contribuiscono all'erogazione dei servizi ICT.

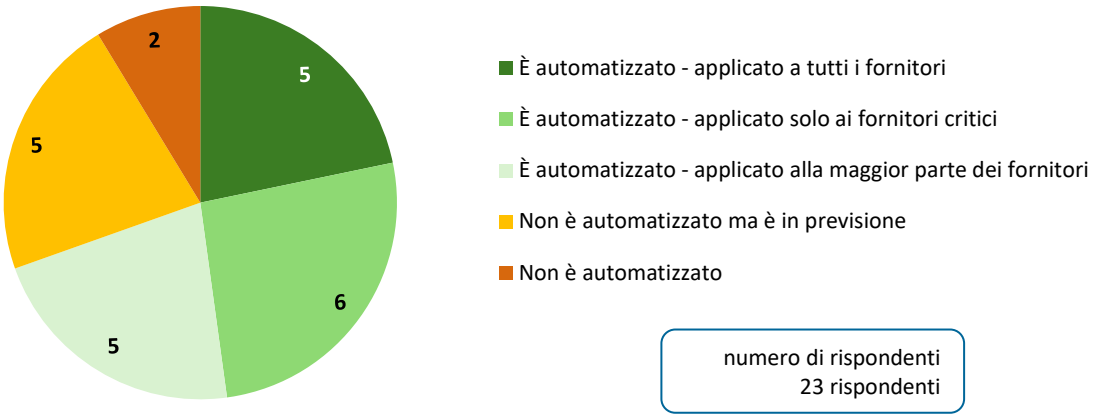
Tale esigenza ha assunto ulteriore rilevanza anche alla luce del Regolamento UE/2022/2554 (Digital Operational Resilience Act, DORA), che pone particolare attenzione alla gestione del rischio derivante dalle terze parti ICT.

In tale contesto, l'utilizzo di strumenti automatizzati rappresenta una modalità evoluta di supporto alle attività di controllo e sorveglianza dei fornitori, consentendo una valutazione più continua e tempestiva del relativo profilo di rischio[5].

Domanda: *Indicare se la banca/gruppo bancario si è dotato di strumenti di monitoraggio automatizzati per valutare il rischio di terze parti (TPRM).*

[5] Esempi di sistemi automatizzati di monitoraggio delle terze parti includono piattaforme di cybersecurity rating, strumenti di monitoraggio delle vulnerabilità e della superficie di attacco esterna, soluzioni per il monitoraggio di incidenti e data breach, nonché applicazioni per il controllo continuo della conformità normativa, delle certificazioni e dei livelli di servizio dei fornitori.

Figura 29 – Gestione del rischio di terze parti



I risultati evidenziano una significativa diffusione degli strumenti di monitoraggio automatizzato per la Gestione del rischio delle terze parti e in prospettiva quasi tutti i rispondenti li introdurranno. Dei 23 rispondenti, 16 dichiarano di aver adottato soluzioni automatizzate. Tali soluzioni risultano applicate esclusivamente ai fornitori critici in sei casi, a tutti i fornitori in cinque casi e alla maggior parte dei fornitori in altri cinque casi.

Un ulteriore gruppo di rispondenti prevede l'introduzione di strumenti di monitoraggio automatizzato in prospettiva (5), mentre risulta limitato il numero di coloro che dichiarano di non aver adottato né pianificato l'automatizzazione degli strumenti (2) (Figura 29).

3.9 Integrazione dei processi e tecnologie a supporto

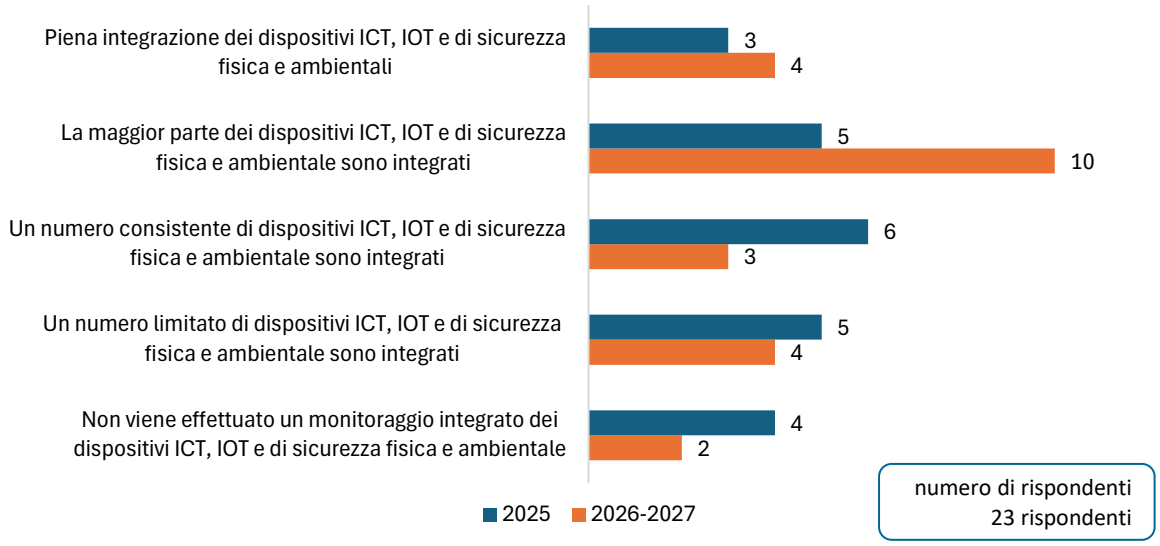
3.9.1 Integrazione sicurezza fisica e logica

La crescente interconnessione tra infrastrutture ICT, dispositivi IoT e sistemi di sicurezza fisica e ambientale rende sempre più rilevante l'adozione di modelli di monitoraggio integrati. Ciò consente una visione più completa degli eventi di sicurezza e favorisce una gestione coordinata dei rischi che possono interessare simultaneamente componenti digitali e fisiche dell'organizzazione.

In tale contesto, l'indagine ha approfondito il livello di integrazione nel monitoraggio delle diverse componenti da parte dei rispondenti e le relative prospettive di evoluzione nel biennio 2026-2027.

Domanda: *Indicare l'assetto prevalente della banca/gruppo in relazione all'integrazione del monitoraggio della sicurezza logica (dispositivi ICT), dei dispositivi IoT e della sicurezza fisica e ambientale, anche in previsione nel biennio 2026-2027.*

Figura 30 – Integrazione sicurezza fisica e logica



I risultati della Figura 30 evidenziano che, nel 2025, la configurazione più segnalata è quella in cui un numero consistente di dispositivi ICT, IoT e di sicurezza fisica e ambientale risulta integrato (6 rispondenti), seguita dai casi in cui la maggior parte dei dispositivi è integrata (5) e da quelli caratterizzati da un'integrazione limitata (5).

Con riferimento al biennio 2026-2027, i rispondenti prevedono un'evoluzione verso assetti maggiormente integrati. In particolare, la configurazione prevalente diventa quella in cui la maggior parte dei dispositivi ICT, IoT e di sicurezza fisica e ambientale risulta integrata (10), mentre si riduce il numero dei rispondenti che rileva l'integrazione di un numero consistente (3) e limitato di dispositivi (4) e l'assenza di monitoraggio integrato (2).

La piena integrazione dei dispositivi ICT, IoT e di sicurezza fisica e ambientale interessa tre rispondenti al 2025 e quattro in previsione nel biennio 2026-2027.

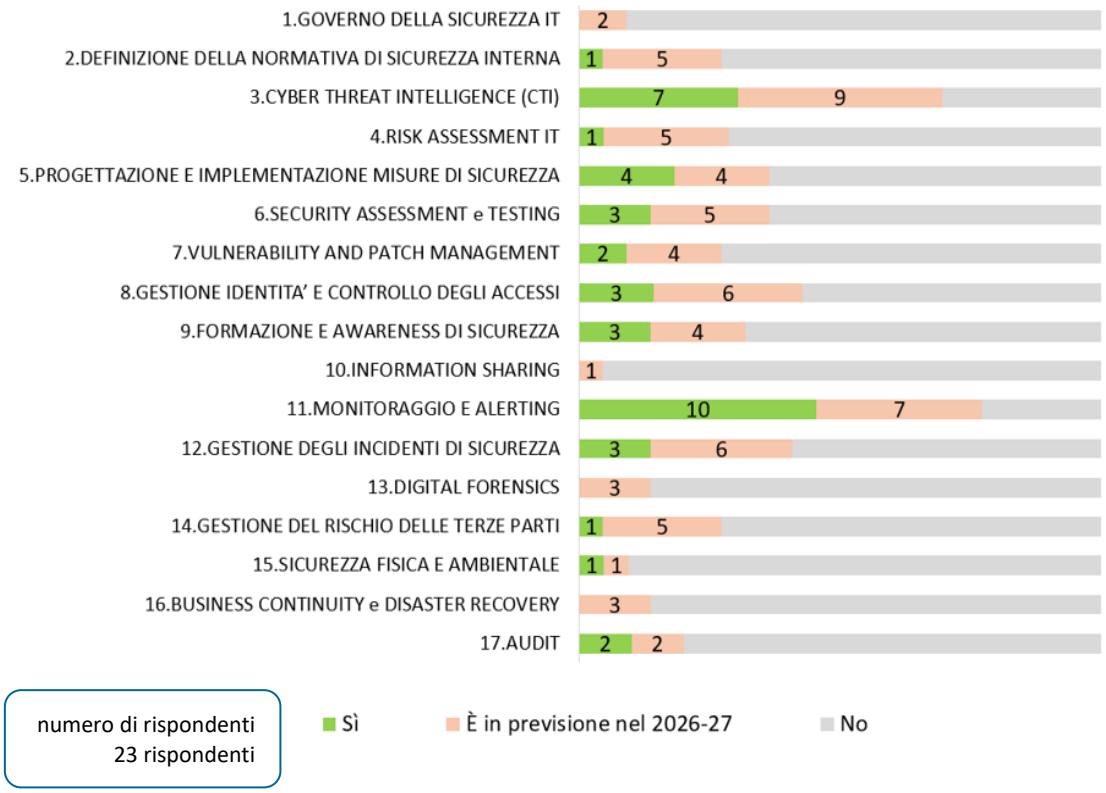
3.9.2 L'Intelligenza Artificiale (IA)

La crescente disponibilità di strumenti basati sull'Intelligenza Artificiale (IA) sta modificando profondamente il panorama della sicurezza informatica, amplificando sia le capacità offensive degli attaccanti sia le modalità di prevenzione, individuazione e risposta adottate dalle organizzazioni.

In tale contesto, l'indagine ha approfondito il grado di utilizzo dell'IA nei principali processi di sicurezza e le iniziative previste dai rispondenti per il biennio 2026-2027.

Domanda: *Indicare in quali dei processi di sicurezza sono utilizzate tecnologie di Intelligenza Artificiale (IA) o ne è previsto l'utilizzo.*

Figura 31 – IA a supporto dei processi di sicurezza



I risultati della Figura 31 evidenziano un crescente interesse verso l'utilizzo dell'Intelligenza Artificiale (IA) a supporto dei processi di sicurezza informatica, sebbene l'adozione risulti al 2025 ancora limitata e concentrata in alcuni ambiti specifici.

Infatti, l'utilizzo dell'IA risulta in particolare nel processo di Monitoraggio e Alerting (10 rispondenti), seguito dalla Cyber Threat Intelligence (7). Livelli di adozione più contenuti si osservano nella Progettazione e implementazione delle misure di sicurezza (4), nelle Attività di Security Assessment e Testing, nella Gestione delle identità e controllo degli accessi, nella Gestione degli incidenti di sicurezza e nella Formazione e Awareness di sicurezza (3). L'utilizzo dell'IA risulta invece marginale o assente negli altri processi considerati, tra cui il Governo della sicurezza IT, l'Information Sharing, la Digital forensics e la Business Continuity e Disaster Recovery.

Con riferimento al biennio 2026-2027, i rispondenti prevedono una significativa estensione dell'uso dell'IA a numerosi processi di sicurezza. Le maggiori prospettive di adozione riguardano la Cyber Threat Intelligence (9), il Monitoraggio e Alerting (7), la Gestione delle identità e controllo degli accessi e la Gestione degli incidenti di sicurezza (6) in aggiunta all'utilizzo dell'IA nel 2025. La crescita è prevista anche nell'ambito del Risk assessment IT (5), della Definizione della normativa di sicurezza interna (5), del Security Assessment e Testing (5) e della Gestione del rischio delle terze parti (5).

Box 5 – IA, nuove capacità di attacco e di difesa

L'Intelligenza Artificiale sta modificando profondamente il panorama della sicurezza informatica, incidendo sia sulle capacità di difesa sia sulle modalità con cui gli attaccanti possono acquisire informazioni e sviluppare nuove tecniche di attacco. In particolare, i

modelli linguistici di grandi dimensioni consentono di rendere accessibili a una platea sempre più ampia conoscenze tecniche che in passato richiedevano competenze specialistiche e tempi di apprendimento più lunghi.

Negli ultimi anni alcuni sistemi di IA sono stati oggetto di interventi finalizzati a limitarne l'utilizzo per attività potenzialmente riconducibili al dominio offensivo della sicurezza informatica. Tali interventi sono stati adottati in seguito alla capacità dei modelli di fornire indicazioni tecniche particolarmente dettagliate su vulnerabilità, configurazioni dei sistemi, strumenti di attacco e procedure operative, evidenziando come l'IA possa contribuire a ridurre le barriere di accesso a conoscenze precedentemente riservate a personale specialistico.

L'utilizzo dell'IA da parte degli attaccanti può inoltre agevolare attività quali l'automazione della ricerca di vulnerabilità, l'analisi di grandi quantità di informazioni pubblicamente disponibili, la produzione di contenuti ingannevoli e il supporto alla preparazione di campagne di attacco più mirate e personalizzate.

Parallelamente, le stesse tecnologie possono essere impiegate a supporto della difesa, favorendo il monitoraggio degli eventi di sicurezza, l'analisi delle minacce, l'individuazione di comportamenti anomali e il supporto alle attività di risposta agli incidenti. L'evoluzione dell'IA tende quindi ad aumentare le capacità operative sia degli attaccanti sia dei difensori, rafforzando l'importanza delle competenze specialistiche, della governance e del continuo aggiornamento dei presidi di sicurezza.

Fonti

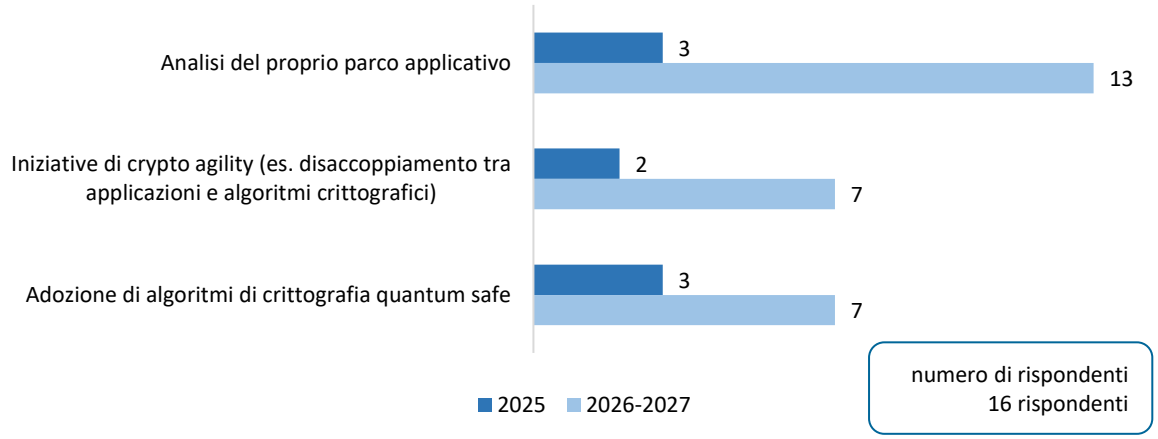
ENISA, Artificial Intelligence and Cyber security
https://www.enisa.europa.eu
NIST, Artificial Intelligence Risk Management Framework (AI RMF)
https://www.nist.gov/itl/ai-risk-management-framework

3.10 Post Quantum Cryptography

In questo paragrafo sono analizzate le principali iniziative avviate o pianificate dai rispondenti in materia di Post Quantum Cryptography, nonché gli strumenti adottati a supporto dell'identificazione e della gestione degli asset crittografici, con l'obiettivo di evidenziare lo stato dell'arte del settore rispetto alla minaccia di sicurezza riguardante l'evoluzione delle tecnologie di computazione quantistica.

Domanda: *Indicare quali delle seguenti iniziative in tema di post quantum cryptography sono state avviate, o si intende avviare nel biennio 2026-2027, per fronteggiare i rischi derivanti dall'uso di algoritmi crittografici (es. RSA, ECDSA) dichiarati vulnerabili ad attacchi condotti con sistemi dotati di capacità di computazione quantistica (Risposta multipla).*

Figura 32 – Post Quantum Cryptography - iniziative

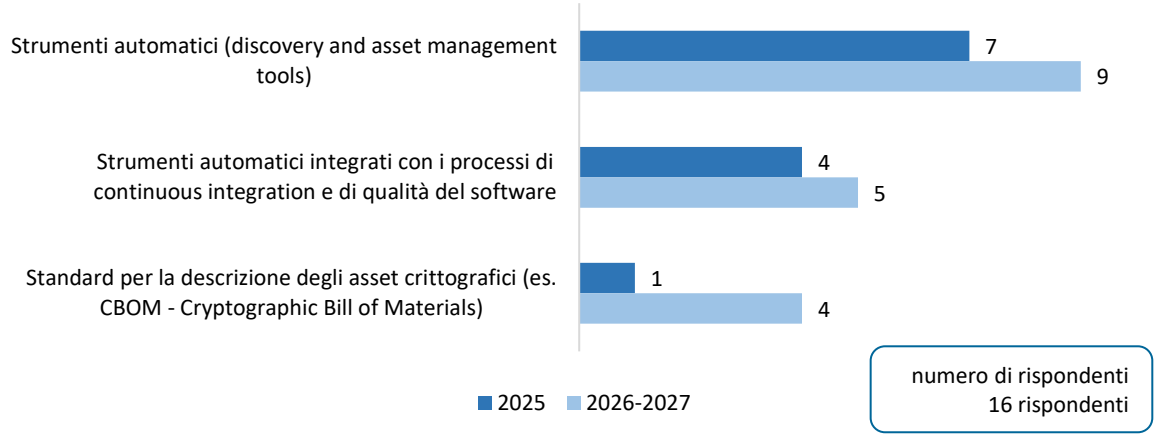


Le iniziative in materia di post quantum cryptography risultano ancora poco diffuse al 2025, ma nel biennio 2026-2027 emerge un significativo incremento. In particolare, l'Analisi del proprio parco applicativo (3 e 13 in prospettiva) rappresenta l'iniziativa maggiormente in crescita per i rispondenti, a conferma dell'importanza attribuita all'identificazione preventiva degli asset e delle componenti crittografiche potenzialmente esposte ai rischi derivanti dall'evoluzione delle capacità di calcolo quantistico.

Una crescita rilevante si osserva anche per le Iniziative di crypto agility (2 e 7 in prospettiva), orientate al disaccoppiamento tra applicazioni e algoritmi crittografici e per l'Adozione di algoritmi di crittografia quantum safe (3 e 7 in prospettiva), evidenziando l'avvio di percorsi di adeguamento volti a rafforzare la resilienza delle infrastrutture crittografiche nel medio periodo (Figura 32).

Domanda: *In caso si siano intraprese iniziative di analisi del proprio parco applicativo, indicare se per tale attività ci si è dotati, o si intende farlo nel biennio 2026-2027, di uno o più dei seguenti strumenti (Risposta multipla).*

Figura 33 – Post Quantum Cryptography - strumenti



Gli strumenti di supporto alle iniziative di transizione verso la crittografia post-quantistica risultano ancora in una fase iniziale di adozione, ma le previsioni per il biennio 2026-2027 evidenziano un progressivo rafforzamento dei relativi presidi. In particolare, gli Strumenti automatici per il censimento e la gestione degli asset (7 e 9 in prospettiva), utilizzati per l'analisi del parco applicativo, risultano i più utilizzati sia nello scenario attuale sia in quello prospettico.

Un utilizzo più contenuto si osserva per gli Strumenti automatici integrati con i processi di continuous integration e di qualità del software (4 e 5 in prospettiva), mentre gli Standard per la descrizione degli asset crittografici, quali il Cryptographic Bill of Materials (CBOM) (1 e 4 in prospettiva), risultano ancora adottati da un numero limitato di rispondenti, pur evidenziando una crescita nelle previsioni per il biennio 2026-2027 (Figura 33).

Box 6 – Osservatorio Quantum Computing

L'Osservatorio Quantum Computing, promosso nell'ambito delle attività della Segreteria Tecnica della CIPA, rappresenta uno spazio permanente di confronto tra banche, autorità e altri soggetti interessati all'evoluzione delle tecnologie quantistiche. L'iniziativa nasce con l'obiettivo di monitorare gli sviluppi tecnologici, favorire la condivisione delle esperienze e accrescere la preparazione del settore bancario rispetto alle opportunità e ai rischi associati al quantum computing.

Dalle prime attività dell'Osservatorio è emerso un livello di maturità eterogeneo tra gli operatori: alcune banche hanno già avviato iniziative di studio, sperimentazione e collaborazione con università e centri di ricerca, mentre altre adottano un approccio prevalentemente esplorativo, orientato alla comprensione dei possibili impatti sul business e sulla sicurezza. Tra i principali temi di interesse figurano le applicazioni del quantum computing nell'ambito dell'Intelligenza Artificiale, del machine learning, dell'ottimizzazione e dell'anomaly detection, oltre agli aspetti legati alla Post-Quantum Cryptography, alla crypto agility e alle sperimentazioni di tecnologie quali la Quantum Key Distribution (QKD).

Un tema centrale delle attività dell'Osservatorio riguarda la preparazione del settore finanziario alla transizione verso soluzioni crittografiche resilienti alle future capacità di calcolo quantistico. In tale ambito è stata presentata la roadmap G7 per la resilienza post-quantum nel sistema finanziario, che individua come passaggio preliminare la predisposizione di un inventario degli asset crittografici e la successiva definizione delle priorità di intervento attraverso attività di analisi del rischio e valutazione dell'impatto.

L'Osservatorio si propone inoltre di favorire il coordinamento tra iniziative nazionali, europee e internazionali, contribuendo alla diffusione di conoscenze e buone pratiche e supportando il settore bancario nell'integrazione delle tematiche quantistiche nei processi di gestione del rischio e di pianificazione strategica. È inoltre prevista la realizzazione di una survey dedicata alle iniziative in corso presso le banche e la pubblicazione periodica di materiali di approfondimento e aggiornamento.

3.11 Ulteriori analisi

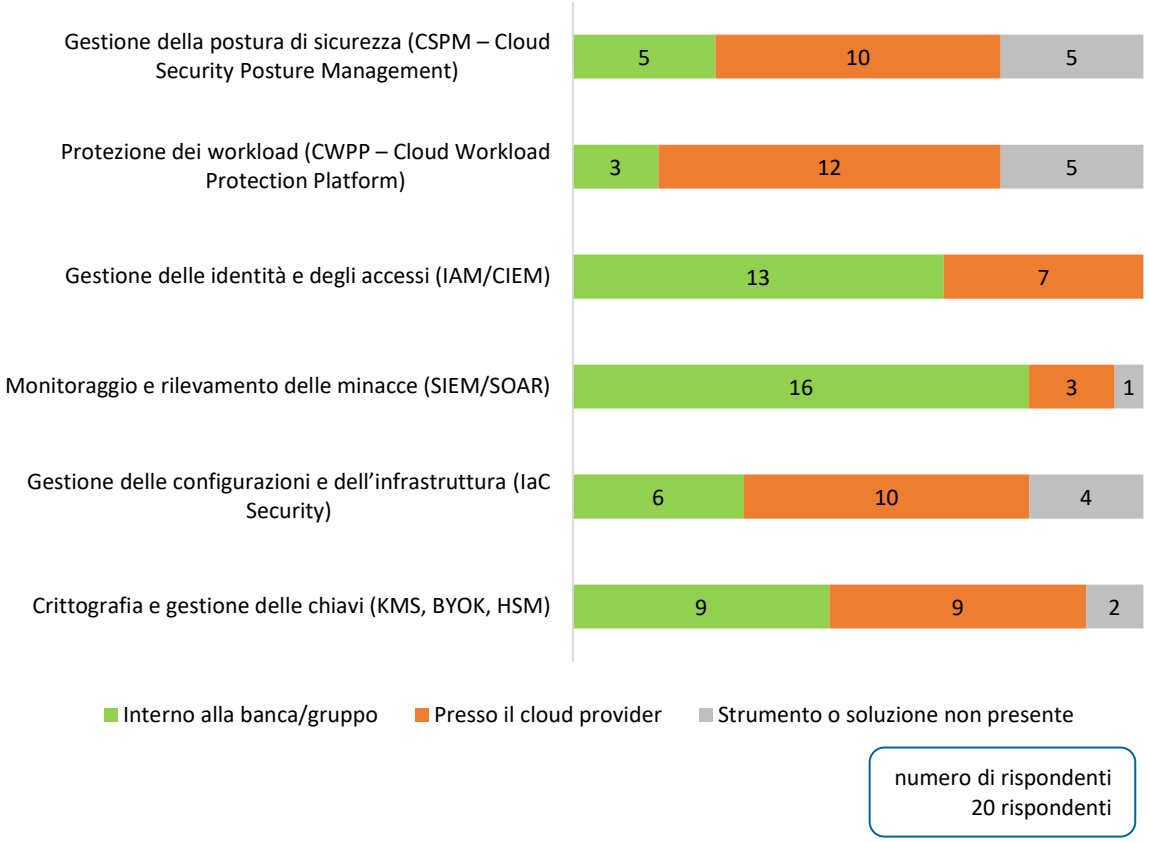
3.11.1 Sicurezza e cloud

La crescente diffusione dei servizi cloud ha determinato un'evoluzione dei modelli di sicurezza adottati dalle banche, rendendo necessario definire in modo chiaro la ripartizione delle responsabilità tra organizzazione e cloud provider.

In tale paragrafo l'analisi approfondisce l'assetto prevalente adottato per i principali strumenti e soluzioni di sicurezza utilizzati nei servizi ICT in public cloud, al fine di evidenziare le modalità di gestione dei relativi presidi.

Domanda: *Indicare per tutti gli strumenti o soluzioni tecniche adottati per la protezione, il monitoraggio e la gestione della sicurezza dei servizi ICT nel public cloud, di seguito elencati, l'assetto prevalente.*

Figura 34 – Assetti per strumenti o soluzioni dei servizi in public cloud



Le modalità di gestione delle principali soluzioni di sicurezza per i servizi ICT in public cloud possono essere diverse in funzione dell'ambito considerato. Nel complesso, i risultati evidenziano un modello nel quale le banche tendono a mantenere all'interno le funzioni maggiormente connesse al monitoraggio delle minacce e alla gestione degli accessi, ricorrendo invece con maggiore frequenza alle soluzioni offerte dai cloud provider per i presidi di sicurezza più strettamente integrati con l'infrastruttura cloud.

In particolare, le attività di Monitoraggio e rilevamento delle minacce tramite SIEM/SOAR risultano prevalentemente gestite internamente alla banca/gruppo (16) così come la Gestione delle identità e degli accessi (IAM/CIEM) (13). Per altri assetti emerge invece un maggiore ricorso alle funzionalità messe a disposizione dal cloud provider. Ciò avviene in particolare per la Protezione dei workload (CWPP) (12), la Gestione delle configurazioni e dell'infrastruttura (IaC Security) (10) e la Gestione della postura di sicurezza (CSPM) (10). Per la Crittografia e gestione delle chiavi (KMS, BYOK, HSM) si osserva un'equa ripartizione tra soluzioni gestite internamente (9) e presso il cloud provider (9).

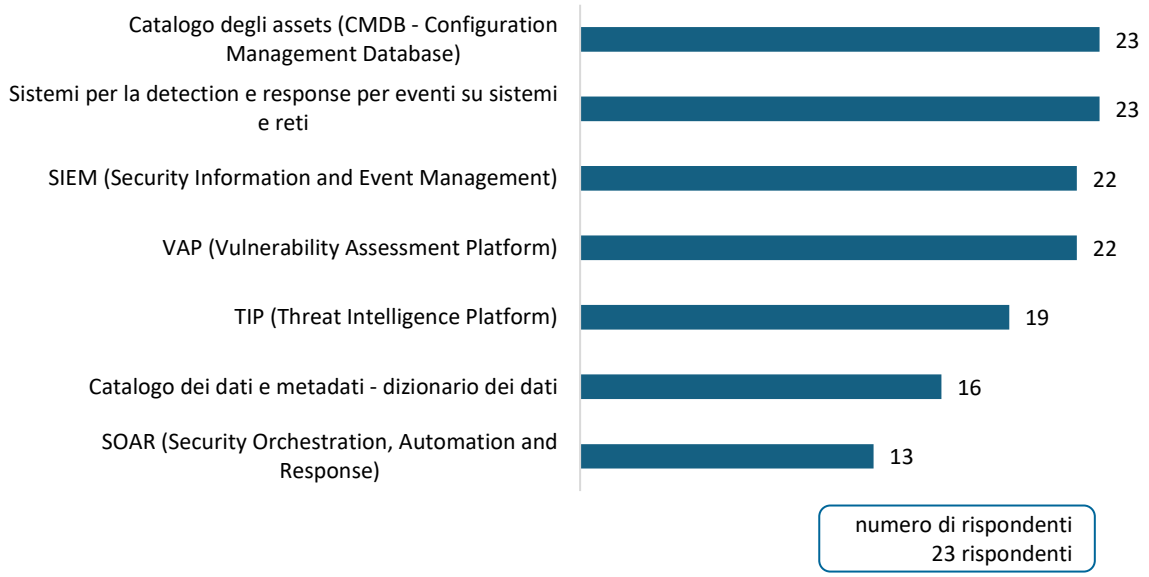
La quota di rispondenti che dichiara l'assenza di specifici strumenti risulta contenuta e interessa principalmente la Protezione dei workload (CWPP) (5), la Gestione della postura di sicurezza (CSPM) (5) e la Gestione delle configurazioni e dell'infrastruttura (IaC Security) (4) (Figura 34).

3.11.2 Strumenti di sicurezza

La disponibilità di adeguati strumenti tecnologici rappresenta un fattore abilitante per l'efficacia dei processi di sicurezza informatica. In questo paragrafo viene analizzato il livello di adozione nel settore bancario dei principali strumenti a supporto delle attività di sicurezza informatica.

Domanda: *Indicare quali tra i seguenti strumenti sono in uso nella banca/gruppo (Risposta multipla).*

Figura 35 – Strumenti in uso



La dotazione tecnologica a supporto dei processi di sicurezza informatica risulta ampiamente consolidata presso i rispondenti. In particolare, tutti dichiarano di disporre di un Catalogo degli assets (CMDB - Configuration Management Database) e di Sistemi per la detection e response per eventi su sistemi e reti (23), mentre quasi tutti fruiscono di piattaforme SIEM (Security Information and Event Management) e VAP (Vulnerability Assessment Platform) (22).

La Threat Intelligence Platform (TIP) (19) e i Cataloghi dei dati e metadati (16), strumenti che contribuiscono rispettivamente al rafforzamento delle attività di analisi della minaccia e alla gestione strutturata del patrimonio informativo, sono comunque ampiamente adottati.

Più contenuta, pur interessando oltre la metà dei rispondenti, risulta la diffusione delle piattaforme SOAR (Security Orchestration, Automation and Response) (13), orientate all'automazione e all'orchestrazione delle attività operative di sicurezza (Figura 35).

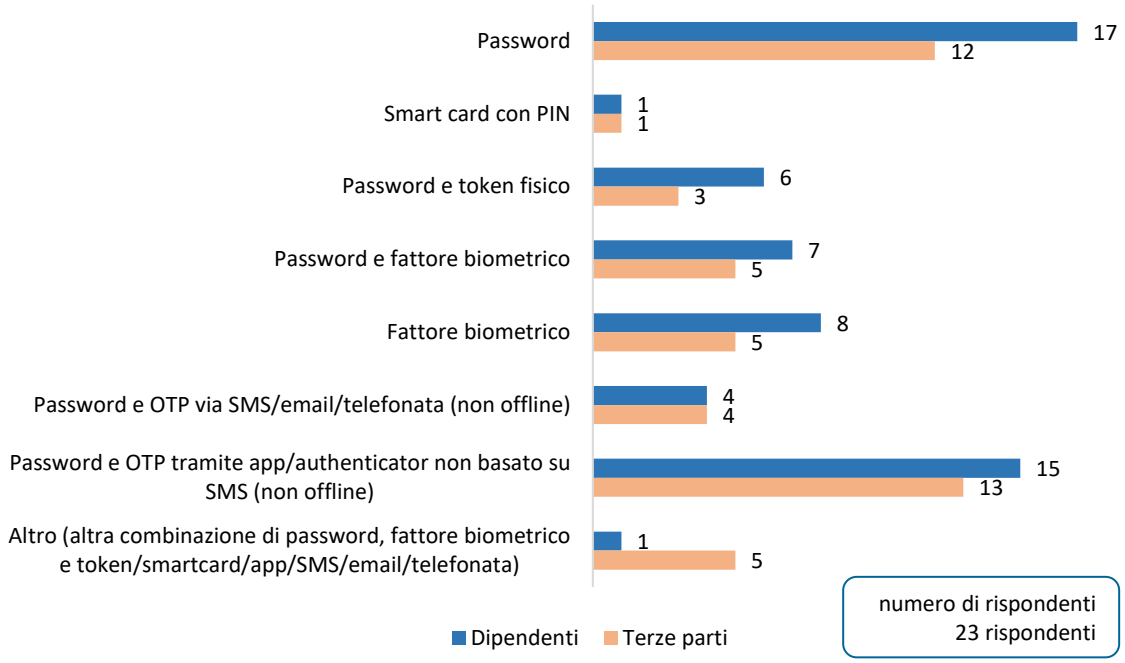
3.11.3 Modalità di autenticazione alla rete aziendale

L'evoluzione delle minacce cyber e la crescente diffusione del lavoro da remoto e dei servizi digitali hanno inoltre favorito l'adozione di meccanismi di autenticazione sempre più robusti, basati sulla combinazione di più fattori di verifica.

In tale contesto, l'indagine ha approfondito le modalità di autenticazione utilizzate per l'accesso ai dispositivi e alla rete aziendale da parte dei dipendenti e delle terze parti.

Domanda: *Indicare la modalità di autenticazione adottata dalla banca/gruppo per l'accesso ai dispositivi aziendali (PC/PC portatili) connessi alla rete da parte dei dipendenti e delle terze parti (es. fornitori, consulenti, collaboratori esterni).*

Figura 36 – Modalità di autenticazione alla rete aziendale



Nel complesso, i risultati evidenziano una maggiore diffusione dell'autenticazione multifattore per gli accessi delle terze parti, mentre per i dipendenti permane un utilizzo significativo delle credenziali tradizionali. Le modalità di autenticazione adottate per l'accesso ai dispositivi aziendali evidenziano una diffusa attenzione verso l'utilizzo di meccanismi di autenticazione multifattore.

Per i dipendenti, la modalità di autenticazione più diffusa è rappresentata dalla Password (17), seguita dalla combinazione Password e OTP tramite app/authenticator non basato su SMS (15). Risulta significativo il ricorso al Fattore biometrico (8) e alla combinazione Password e fattore biometrico (7), mentre Password e token fisico è adottata da sei rispondenti. Più contenuto risulta invece l'utilizzo delle altre modalità di autenticazione (1).

Per le terze parti, la modalità maggiormente utilizzata è la combinazione Password e OTP tramite app/authenticator non basato su SMS (13), seguita dalla Password (12). Sono inoltre adottati il Fattore biometrico (5), la combinazione Password e fattore biometrico (5) e altre modalità di autenticazione (5) (Figura 36).

Capitolo 4. Identità digitale

Il presente capitolo analizza le prospettive di evoluzione dell'identità digitale nel settore bancario, con particolare riferimento all'adozione degli EUDI (European Digital Identity) Wallet e delle Attestazioni Elettroniche di Attributi (EAA), nell'ambito del quadro normativo introdotto dal Regolamento UE/2024/1183 (Electronic Identification, Authentication and Trust Services, eIDAS2).

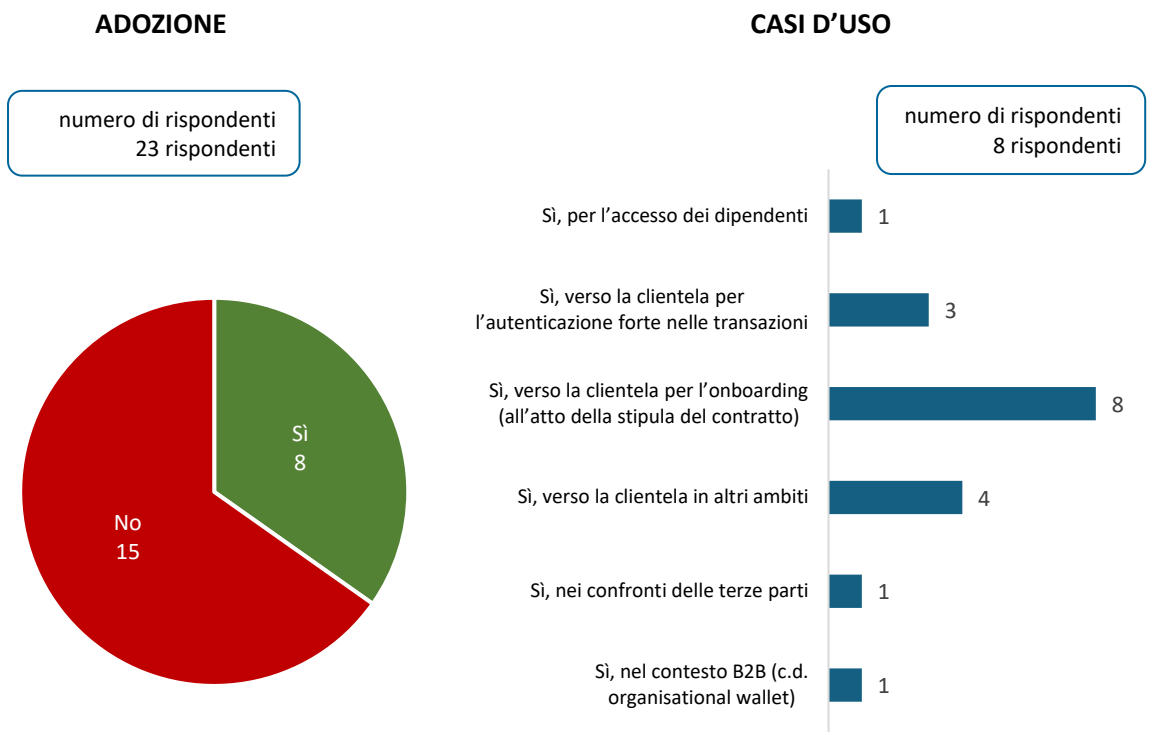
L'analisi approfondisce la roadmap e le principali iniziative previste dai rispondenti, esaminando gli ambiti applicativi maggiormente interessati, le modalità di sviluppo che saranno adottate, la partecipazione a iniziative europee e i possibili servizi che utilizzeranno tali strumenti. In questo ambito, in particolare, il capitolo esamina le modalità di autenticazione attualmente utilizzate e le prospettive evolutive connesse all'introduzione degli EUDI Wallet nei servizi rivolti alla clientela.

4.1 Adozione e ambiti di utilizzo degli EUDI Wallet

L'evoluzione del quadro normativo europeo in materia di identità digitale sta aprendo nuove opportunità di innovazione per il settore bancario. Gli EUDI Wallet e le EAA potranno infatti supportare nuovi modelli di identificazione e autenticazione della clientela, oltre ad abilitare modalità più efficienti di scambio e verifica delle informazioni. In questo paragrafo vengono analizzate le roadmap di adozione eventualmente definite dai rispondenti e i principali ambiti applicativi nei quali è previsto l'utilizzo di tali strumenti.

Domanda: *Indicare se è definita una roadmap nella banca/gruppo per l'utilizzo degli EUDI Wallet come regime di autenticazione (Risposta multipla).*

Figura 37 – Roadmap di adozione e casi di utilizzo degli EUDI Wallet



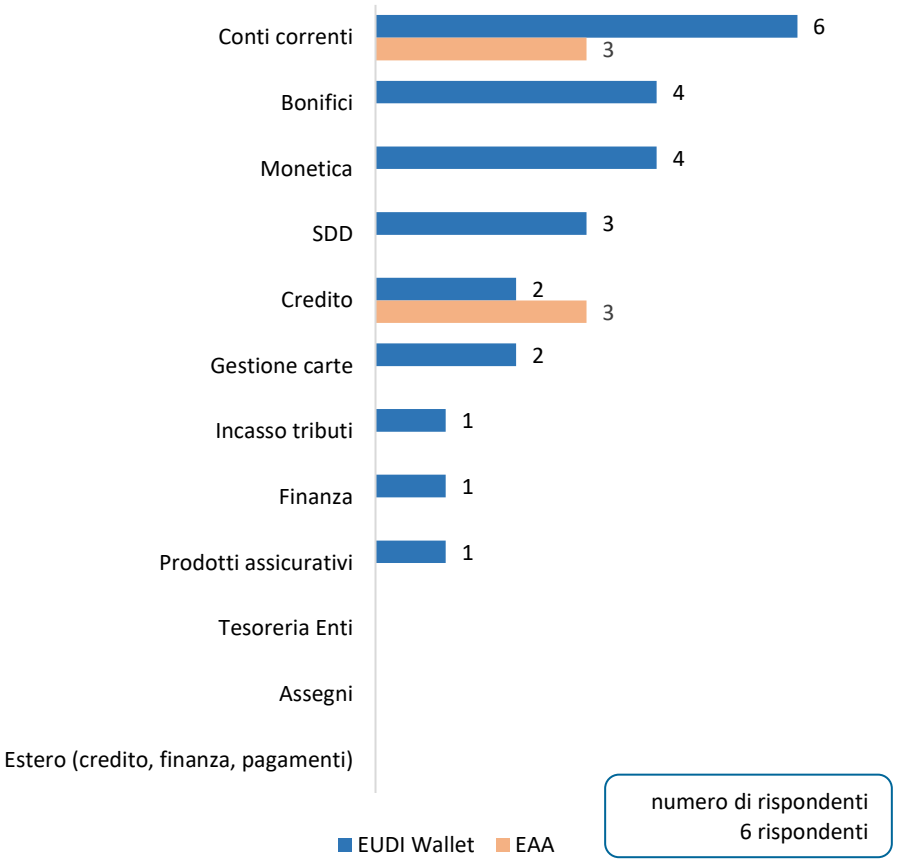
Dall'indagine emerge che otto dei 23 rispondenti hanno definito una roadmap per l'utilizzo degli EUDI Wallet.

I rispondenti che hanno definito una roadmap prevedono tutti l'utilizzo degli EUDI Wallet nell'ambito dell'onboarding della clientela (8), quattro ne prevedono anche l'impiego verso la clientela in Altri ambiti e tre per l'Autenticazione forte nelle transazioni.

Risultano invece ancora limitati i casi di utilizzo previsti per l'Accesso dei dipendenti, nei confronti delle terze parti e nel contesto B2B, attraverso l'impiego dell'Organisational wallet (1) (Figura 37).

***Domanda**: Con riferimento alla mappa applicativa ABI Lab, quali ambiti sono o saranno interessati dagli EUDI Wallet e, qualora si esercitasse anche il ruolo di fonte autentica, dall'emissione di "Attestazioni Elettroniche di Attributi" (EAA) nei confronti di terzi.*

Figura 38 – Ambiti di utilizzo degli EUDI Wallet e delle EAA



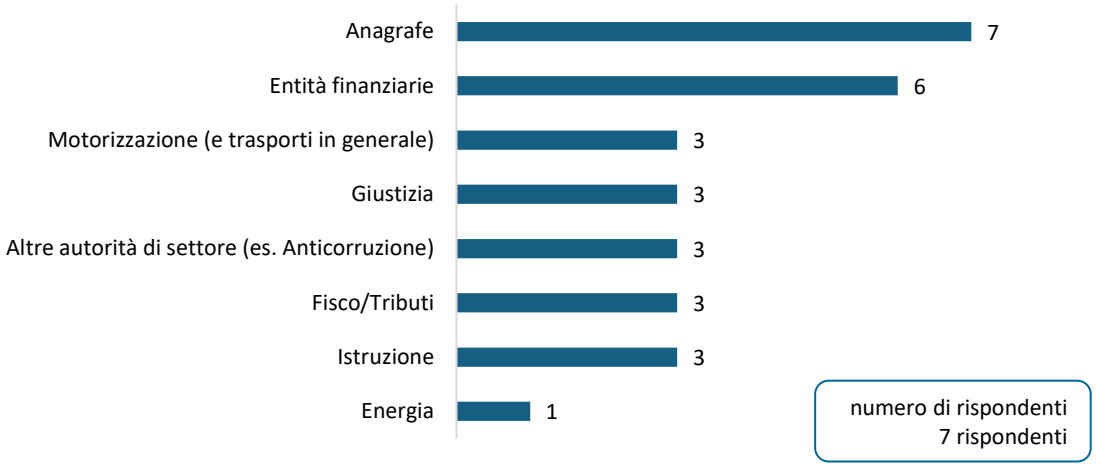
I risultati evidenziano che gli ambiti maggiormente interessati dagli EUDI Wallet risultano i Conti correnti (6), seguiti dai Bonifici e dalla Monetica (4). Per tre rispondenti è segnalato interesse per gli SDD, mentre risultano più limitati gli utilizzi previsti negli ambiti del Credito, della Gestione carte (2), della Finanza, dell'Incasso tributi e dei Prodotti assicurativi (1).

Con riferimento alle EAA, gli ambiti indicati dai rispondenti sono i Conti correnti e il Credito (3).

Nel complesso, i risultati mostrano come le principali opportunità di applicazione degli EUDI Wallet e delle EAA siano attualmente individuate nei servizi bancari maggiormente connessi all'identificazione della clientela e alla gestione della relazione commerciale. In particolare, l'onboarding e i servizi di conto corrente sembrano rappresentare i contesti nei quali tali strumenti potrebbero generare i maggiori benefici in termini di semplificazione dei processi, affidabilità delle informazioni e interoperabilità con il futuro ecosistema europeo dell'identità digitale (Figura 38).

Domanda: *Nel caso in cui la banca/gruppo decidesse di accettare "Attestazioni Elettroniche di Attributi" (EAA) da soggetti terzi, indicare quali settori di provenienza sarebbero interessati.*

Figura 39 – Settori di provenienza per le EAA



I risultati evidenziano che l'interesse verso le Attestazioni Elettroniche di Attributi (EAA) è concentrato principalmente sulle informazioni provenienti dall'Anagrafe (7) e dalle Entità finanziarie (6). Sono segnalati da tre rispondenti anche i seguenti ambiti: Istruzione, Fisco/Tributi, Altre autorità di settore, Giustizia e Motorizzazione.

Più contenuto risulta invece l'interesse per gli attributi provenienti dal settore Energia (1) (Figura 39).

Box 7 – EUDI Wallet e Attestazioni Elettroniche di Attributi (EAA)

L'identità digitale europea

Il Regolamento UE/2024/1183 (Electronic Identification, Authentication and Trust Services, eIDAS2), che modifica il Regolamento UE/910/2014 (Electronic Identification, Authentication and Trust Services, eIDAS), introduce l'European Digital Identity Wallet (EUDI Wallet), uno strumento che consentirà a cittadini e imprese di identificarsi e autenticarsi online attraverso un'identità digitale riconosciuta in tutti gli Stati membri dell'Unione europea. Gli EUDI Wallet inoltre consentiranno di richiedere, conservare e condividere in modo sicuro importanti documenti digitali personali, nonché di firmare o sigillare elettronicamente documenti. Essi potranno favorire l'accesso a servizi pubblici e privati, garantendo maggiore interoperabilità, controllo dei dati personali e uniformità delle modalità di identificazione digitale a livello europeo.

Le attestazioni elettroniche di attributi

Gli Electronic Attestations of Attributes (EAA) sono attestazioni rilasciate in formato elettronico che consentono di certificare specifici attributi relativi a persone fisiche o giuridiche o oggetti. Tali attributi possono riguardare, ad esempio:

- *dati anagrafici;*
- *titoli di studio;*
- *qualifiche professionali;*
- *informazioni fiscali;*
- *titolarità di rapporti bancari;*
- *altri attributi provenienti da fonti autentiche pubbliche o private.*

Le EAA consentono di condividere soltanto le informazioni strettamente necessarie per l'accesso a uno specifico servizio, secondo il principio della minimizzazione dei dati previsto dalla normativa europea in materia di protezione dei dati personali.

Possibili applicazioni nel settore bancario

Nel settore bancario gli EUDI Wallet e le EAA potranno supportare numerosi processi, tra cui:

- *onboarding e identificazione della clientela;*
- *autenticazione per l'accesso ai servizi digitali;*
- *verifica di requisiti e attributi della clientela;*
- *sviluppo di nuovi servizi digitali interoperabili a livello europeo.*

L'introduzione di tali strumenti potrebbe contribuire a semplificare i processi di identificazione e autenticazione, favorendo al tempo stesso una maggiore sicurezza e affidabilità nella gestione delle identità digitali.

Fonti

Regolamento UE/910/2014 (Electronic Identification, Authentication and Trust Services, eIDAS)
https://eur-lex.europa.eu/eli/reg/2014/910/oj
Regolamento UE/2024/1183 (Electronic Identification, Authentication and Trust Services, eIDAS2)
https://eur-lex.europa.eu/eli/reg/2024/1183/oj
Commissione europea
https://digital-strategy.ec.europa.eu/en/policies/european-digital-identity
European Digital Identity Framework
https://digital-strategy.ec.europa.eu/en/policies/european-digital-identity
European Union Toolbox for the EU Digital Identity Wallet
https://digital-strategy.ec.europa.eu/en/library/eu-toolbox-digital-identity-wallet

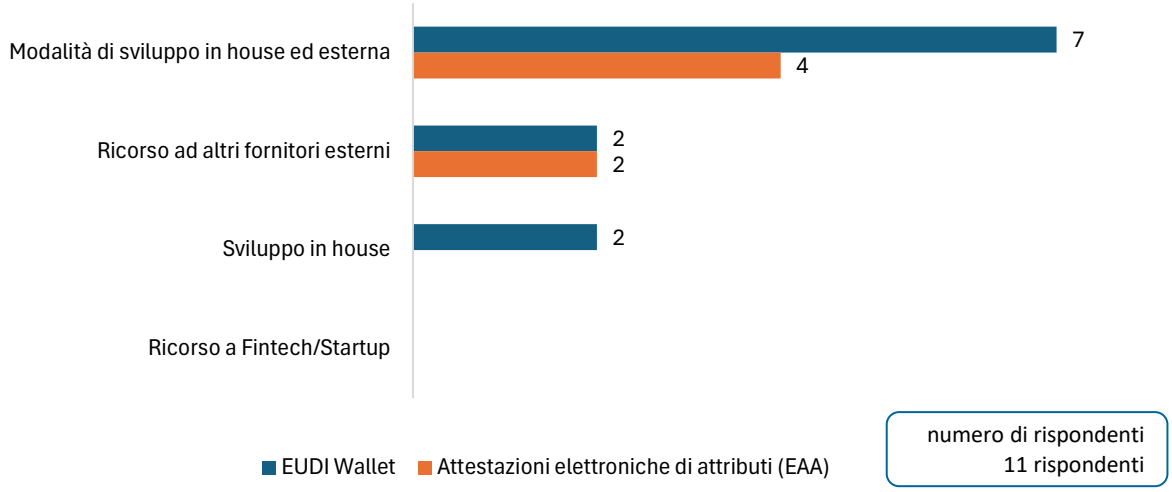
4.2 Modelli di sviluppo

L'evoluzione dell'identità digitale richiede l'individuazione delle modalità organizzative e tecnologiche più idonee per la realizzazione delle soluzioni.

In tale contesto, l'indagine ha approfondito i modelli di sviluppo previsti dai rispondenti per le iniziative connesse agli EUDI Wallet e alle EAA, al fine di comprendere il ruolo delle competenze interne e il ricorso a soggetti esterni specializzati nello sviluppo delle relative soluzioni. Ha inoltre analizzato il ricorso alla Distributed Ledger Technology.

Domanda: *Indicare le modalità di sviluppo a cui la banca/gruppo ricorre nel caso di soluzioni legate all'uso di EUDI Wallet e/o "Attestazioni Elettroniche di Attributi" (EAA).*

Figura 40 – Modalità di sviluppo



I risultati evidenziano che i rispondenti che adottano soluzioni basate su EUDI Wallet privilegiano modalità di sviluppo che combinano competenze in house ed esterne (7). Più contenuto risulta il ricorso esclusivo allo sviluppo in house (2) e ad altri fornitori esterni (2), mentre non si rilevano casi di sviluppo basati esclusivamente sul ricorso a Fintech o Startup.

Anche per le soluzioni relative alle EAA prevale la modalità di sviluppo mista (in house ed esterna) (4), mentre il ricorso esclusivo a fornitori esterni interessa due rispondenti (Figura 40).

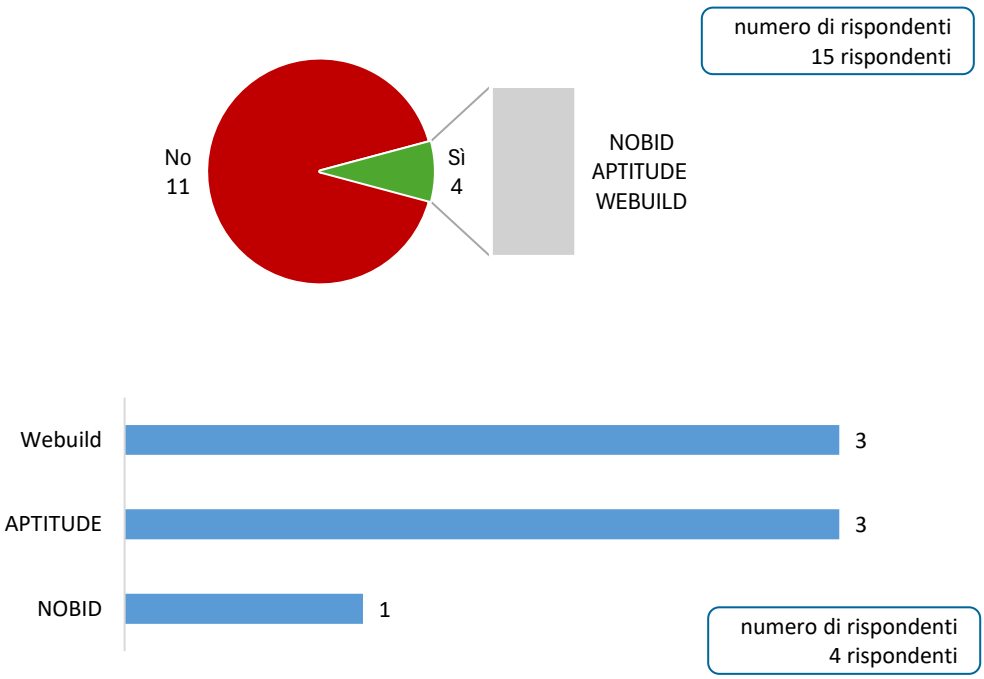
Con riferimento all'utilizzo della DLT (Distributed Ledger Technology) per lo sviluppo di EUDI Wallet e/o EAA, dalle analisi risulta che un solo rispondente ne prevede l'impiego. Ne consegue che la DLT non sembra al momento essere considerata un elemento centrale nelle strategie di sviluppo delle soluzioni di identità digitale nel settore.

4.3 Partecipazione a iniziative europee

Con riferimento all'ecosistema degli EUDI Wallet, in questo paragrafo sono analizzate le iniziative a livello europeo alle quali le banche partecipano.

Domanda: *Indicare se la banca/gruppo aderisce a iniziative a livello europeo per lo sviluppo dell'ecosistema degli EUDI Wallet (es. progetti pilota su vasta scala).*

Figura 41 – Adesione a iniziative a livello europeo per EUDI Wallet



La partecipazione a iniziative europee per lo sviluppo dell'ecosistema degli EUDI Wallet risulta ancora circoscritta a un numero limitato di rispondenti. In particolare, soltanto quattro dichiarano di aderire a progetti di livello europeo, mentre la maggior parte (11) non partecipa attualmente ad alcuna iniziativa di questo tipo.

Tra le banche coinvolte emerge un'adesione prevalente ai progetti APTITUDE e WEBUILD, indicati da tre rispondenti, mentre uno dichiara di partecipare alle iniziative NOBID. Da un'ulteriore analisi il partecipante a NOBID partecipa anche a WEBUILD e APTITUDE (Figura 41).

Box 8 – I principali progetti pilota europei su EUDI Wallet

NOBID (Nordic-Baltic eID Project) *è un'iniziativa europea che contribuisce alla sperimentazione del futuro ecosistema dell'identità digitale europea attraverso casi d'uso concreti e scenari operativi transfrontalieri. Il progetto riunisce amministrazioni pubbliche, operatori privati e fornitori di servizi digitali con l'obiettivo di verificare l'effettiva interoperabilità degli* ***EUDI Wallet*** *tra differenti Paesi e contesti applicativi.*

Le attività sviluppate nell'ambito NOBID sono orientate a comprendere come le future identità digitali europee possano essere utilizzate nella vita quotidiana di cittadini e imprese, favorendo modalità sicure e standardizzate di identificazione, autenticazione e condivisione di attributi certificati. I risultati delle sperimentazioni costituiscono un importante contributo alla definizione delle future modalità di utilizzo degli EUDI Wallet in Europa.

APTITUDE (Authentication and Payments in a Trusted Digital Environment) *è un progetto pilota europeo finalizzato a sperimentare l'utilizzo dell'identità digitale europea in contesti*

*caratterizzati da elevati requisiti di sicurezza, fiducia e interoperabilità. L'iniziativa contribuisce alla realizzazione del futuro ecosistema degli **EUDI Wallet**, verificando come le credenziali digitali europee possano essere impiegate nei processi di identificazione, autenticazione e autorizzazione all'interno di servizi pubblici e privati.*

*Le attività di sperimentazione sono orientate a valutare l'integrazione degli **EUDI Wallet** nei servizi finanziari e nei pagamenti digitali, analizzandone i potenziali benefici in termini di semplificazione dell'esperienza utente, maggiore affidabilità delle informazioni e interoperabilità tra soggetti appartenenti a differenti Paesi dell'Unione europea. I risultati del progetto contribuiscono alla definizione di modelli organizzativi e tecnologici a supporto della futura diffusione dell'identità digitale europea.*

***WEBUILD (Wallet Ecosystem for Business and Digital Identity)** è un progetto pilota europeo che contribuisce alla realizzazione dell'ecosistema dell'identità digitale europea attraverso la sperimentazione di casi d'uso che coinvolgono cittadini, imprese e fornitori di servizi. L'iniziativa nasce con l'obiettivo di verificare come gli **EUDI Wallet** possano essere utilizzati in contesti operativi differenti, promuovendo interoperabilità, fiducia e riconoscimento reciproco delle identità digitali tra i Paesi dell'Unione europea.*

Le attività sviluppate nell'ambito del progetto sono orientate a comprendere come credenziali digitali e attestazioni elettroniche di attributi possano supportare l'accesso ai servizi, la condivisione sicura delle informazioni e le interazioni tra organizzazioni pubbliche e private. Le sperimentazioni contribuiscono inoltre alla definizione di modelli tecnologici e operativi destinati a favorire la futura diffusione degli EUDI Wallet e dei servizi di identità digitale a livello europeo.

Fonti

Commissione europea, European Digital Identity Wallet – Large Scale Pilots
https://digital-strategy.ec.europa.eu/en/policies/eudi-wallet-implementation
NOBID Consortium
https://nobidconsortium.com/
APTITUDE Consortium
https://aptitude.digital-identity-wallet.eu/
WEBUILD Consortium
https://www.webuildconsortium.eu/

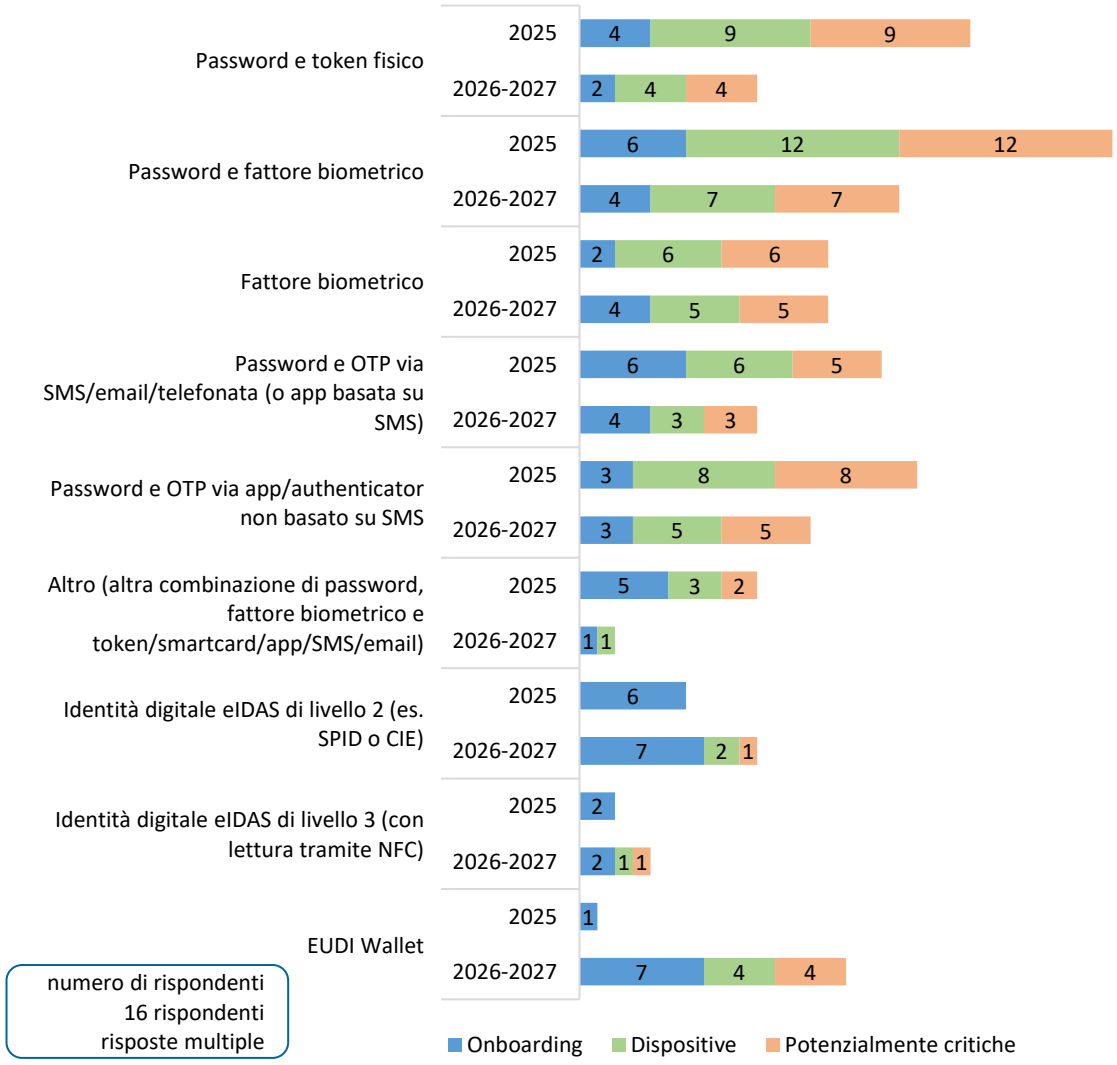
4.4 Modalità di autenticazione nei servizi alla clientela

L'evoluzione del quadro normativo europeo in materia di identità digitale e la crescente diffusione di meccanismi di autenticazione avanzati stanno favorendo lo sviluppo di soluzioni in grado di coniugare sicurezza, semplicità di utilizzo e interoperabilità tra differenti servizi e piattaforme.

In tale contesto, l'indagine ha approfondito le modalità di identificazione/autenticazione attualmente utilizzate e quelle previste nel biennio 2026-2027 per i processi di onboarding della clientela, le operazioni dispositive e le operazioni potenzialmente critiche, con particolare attenzione al ruolo delle identità digitali conformi al Regolamento UE/2024/1183 (Electronic Identification, Authentication and Trust Services, eIDAS2) e alle prospettive di adozione degli EUDI Wallet.

***Domanda**: Con riferimento ai servizi forniti alla clientela e alle tipologie di operazioni in legenda, indicare le modalità di identificazione autenticazione adottate anche in prospettiva con l'utilizzo di EUDI Wallet.*

Figura 42 – Modalità di identificazione/autenticazione per i servizi forniti alla clientela



L'analisi evidenzia nel complesso una progressiva evoluzione verso forme di identificazione/autorizzazione digitale coerenti con lo sviluppo del quadro europeo dell'identità digitale.

In particolare, nel 2025 prevalgono le soluzioni tradizionali basate sulla combinazione di password e fattore biometrico, utilizzate da 12 rispondenti, sia per le operazioni dispositive sia per quelle potenzialmente critiche e da sei per le attività di onboarding.

I risultati evidenziano inoltre come nel 2025 siano già presenti i primi segnali di evoluzione verso modelli di identità digitale più avanzati. In particolare, l'identità digitale eIDAS di livello 2 (es. SPID o CIE) è già prevista da sei rispondenti per i processi di onboarding, mentre un utilizzo degli EUDI Wallet, seppur ancora limitato, è già segnalato da un rispondente.

In prospettiva, nel biennio 2026-2027, si osserva generalmente una riduzione dell'utilizzo delle principali modalità di autenticazione tradizionali. Contestualmente aumenta il ricorso all'identità digitale eIDAS di livello 2, che passa da sei a sette rispondenti per i processi di onboarding, e cresce in modo significativo l'utilizzo degli EUDI Wallet, previsti da sette rispondenti per l'onboarding della clientela e da 4, sia per le operazioni dispositive sia per quelle potenzialmente critiche.

Più contenuta risulta invece la diffusione dell'identità digitale eIDAS di livello 3, che interessa un numero limitato di rispondenti sia nello scenario attuale sia in quello prospettico (2 e 4 rispettivamente).

Nel complesso l'onboarding della clientela risulta l'ambito nel quale si concentra maggiormente l'interesse per l'adozione degli EUDI Wallet, sia nello scenario attuale sia in quello prospettico (Figura 42).

Indice delle figure

Figura 1 – Rappresentatività del campione dei gruppi per totale attivo 5
Figura 2 – Strategia aziendale per la sicurezza informatica 9
Figura 3 – Tematiche di sicurezza indirizzate nella strategia 10
Figura 4 – Figure coinvolte nella definizione della strategia di sicurezza.....11
Figura 5 – Figura CISO formalizzata 12
Figura 6 – Livello di maturità e iniziative progettuali nei processi di sicurezza.....14
Figura 7 – Iniziative progettuali nei processi di sicurezza.....15
Figura 8 – Tipologie di iniziative.....16
Figura 9 – Collocazione organizzativa delle funzioni di sicurezza.....17
Figura 10 – Metodologia per la rilevazione dei costi.....19
Figura 11 – Budget IT 2026 - tipologia di stanziamento 20
Figura 12 – Competenze IT: AS IS e TO BE 21
Figura 13 – Competenze: AS IS e TO BE 22
Figura 14 – GAP di competenze 23
Figura 15 – Modalità di reperimento competenze.....24
Figura 16 – Requisiti per l'assunzione di esperti in sicurezza informatica 25
Figura 17 – Ricorso a istituti di formazione 26
Figura 18 – Certificazioni professionali di riferimento 26
Figura 19 – Organismi di riferimento considerati.....27
Figura 20 – Destinatari della formazione in sicurezza informatica 28
Figura 21 – Minacce cyber considerate nel Risk assessment IT 29
Figura 22 – Processi di sicurezza e rischi del contesto geopolitico 30
Figura 23 – Cyber Threat Intelligence – Valutazione strategica 31
Figura 24 – Cyber Threat Intelligence – Valutazione tattico-operativa.....32
Figura 25 – Information Sharing – Partecipazione a iniziative 33
Figura 26 – Security Assessment – Red Teaming.....35
Figura 27 – Vulnerability Assessment e Patch Management 37
Figura 28 – Definizione policy di Forensic Readiness 38
Figura 29 – Gestione del rischio di terze parti 39
Figura 30 – Integrazione sicurezza fisica e logica 40
Figura 31 – IA a supporto dei processi di sicurezza 41
Figura 32 – Post Quantum Cryptography - iniziative.....43
Figura 33 – Post Quantum Cryptography - strumenti 43
Figura 34 – Assetti per strumenti o soluzioni dei servizi in public cloud.....45
Figura 35 – Strumenti in uso.....46
Figura 36 – Modalità di autenticazione alla rete aziendale.....47
Figura 37 – Roadmap di adozione e casi di utilizzo degli EUDI Wallet 50
Figura 38 – Ambiti di utilizzo degli EUDI Wallet e delle EAA 51
Figura 39 – Settori di provenienza per le EAA 52
Figura 40 – Modalità di sviluppo.....54
Figura 41 – Adesione a iniziative a livello europeo per EUDI Wallet.....55
Figura 42 – Modalità di identificazione/autenticazione per i servizi forniti alla clientela ..57