Osservatorio ACCREDIA
1 2022

Cybersecurity e protezione dei dati: il ruolo della certificazione accreditata

Executive Summary

In collaborazione con:
CYBERSECURITY NATIONAL LAB

ACCREDIA
L'ENTE ITALIANO DI ACCREDITAMENTO

Osservatorio Accredia

Direttore editoriale
Gianluca Di Giulio

Coordinamento editoriale
Alessandro Nisi
Francesca Nizzero

Realizzazione grafica
ZERO ONE

Il presente documento è l'Executive Summary dello studio realizzato dall'Osservatorio congiunto "Cybersecurity e Certificazione" costituito da Accredia e dal Cybersecurity National Lab del Consorzio Interuniversitario Nazionale per l'Informatica (CINI).

Per Accredia: gruppo di lavoro coordinato dall'area Relazioni Istituzionali ed Esterne - Studi e Statistiche e composto da Riccardo Bianconi, Amerigo Cancellieri, Gianluca Di Giulio, Lorenza Guglielmi, Alessandro Nisi, Guglielmo Tozzi, Pietro Vitaliano, Alessandra Zacchetti.

Per il Cybersecurity National Lab: gruppo di lavoro diretto da Alessandro Armando e composto da Francesco Buccafurri, Fabio De Rosa, Giorgio Giacinto, Paolo Prinetto, Leonardo Querzoni, Luca Verderame.

ACCREDIA
L'Ente Italiano di Accreditamento

Via Guglielmo Saliceto, 7/9
00161 Roma

Tel. +39 06 844099.1
Fax. +39 06 8841199

info@accredia.it
www.accredia.it

Cybersecurity e protezione dei dati: il ruolo della certificazione accreditata

La cybersecurity ha assunto un ruolo di primo piano nell'agenda di Governi, Istituzioni e aziende, rientrando tra le priorità dei paesi dell'Unione europea. Con lo sviluppo della società digitale e la pervasività dei servizi ICT, il tema della cybersecurity ha assunto un ruolo strategico; si tratta di una questione da affrontare con serietà, per garantire la giusta protezione di dati, applicazioni e sistemi, da parte di ogni tipo di organizzazione, sia pubblica sia privata, ma anche dei singoli cittadini. Ad accrescere l'importanza della problematica concorre il fatto che oggi molte infrastrutture critiche su scala nazionale sono gestite attraverso sistemi informatici che possono diventare oggetto di attacchi e i cui effetti possono compromettere l'erogazione di servizi di utilità pubblica.
Le analisi contenute nello studio dell'Osservatorio Accredia "Cybersecurity e protezione dei dati: il ruolo della certificazione accreditata" forniscono utili elementi a supporto del principio secondo il quale le valutazioni della conformità alle norme tecniche, irrobustitite con l'accreditamento, rappresentano fattori abilitanti per la cybersecurity, esercitando un ruolo determinante nell'attuale processo di trasformazione digitale della società.

Il contesto normativo

In Europa la Direttiva sulla sicurezza delle reti e delle informazioni (Direttiva EU 2016/1148) nota come NIS[1] (*Network and Information Security*) è stata il primo "pezzo" di legislazione sulla cybersecurity a livello UE, con l'obiettivo di migliorare la sicurezza informatica e delle informazioni in tutta l'Unione. Venivano imposti ai Paesi membri una serie di obblighi, tradotti in misure di sicurezza, per conseguire un livello comune elevato di sicurezza della rete e dei sistemi informativi. In particolare, la Direttiva imponeva agli Stati membri di adottare una strategia nazionale, stabilendo obblighi di sicurezza aggiuntivi e di notifica per gli operatori di servizi essenziali e per i fornitori di servizi digitali. Con la stessa Direttiva si faceva obbligo agli Stati membri di designare Autorità nazionali competenti, punti di contatto unici e *Computer Security Incident Response Team* (CSIRT) con compiti connessi alla cybersecurity.

[1] *Oggi la proposta di una nuova Direttiva EU NIS2 rientra in un pacchetto di misure della Commissione europea volte a migliorare ulteriormente le capacità di resilienza e di risposta agli incidenti di soggetti pubblici e privati, delle autorità competenti e dell'Unione nel suo complesso, nel campo della cybersicurezza e della protezione delle infrastrutture critiche. La bozza della nuova Direttiva comprende una nuova strategia per la cybersecurity, che mira a rafforzare l'autonomia strategica dell'Unione al fine di migliorarne la resilienza (soprattutto degli operatori critici di servizi essenziali) e la risposta collettiva agli incidenti cyber.*

Più recentemente il Regolamento UE 2019/881, cosiddetto *Cybersecurity Act*, costituisce una parte fondamentale della nuova strategia dell'UE per la sicurezza cibernetica, mirando a rafforzare la resilienza dell'Unione agli attacchi informatici e a creare un mercato unico della sicurezza cibernetica in termini di prodotti, servizi e processi ICT. Il fine è accrescere la fiducia dei consumatori nelle tecnologie digitali.
Un primo punto chiave del Regolamento riguarda il rafforzamento del ruolo della *European Union Agency for Cybersecurity* (ENISA)[2]. In particolare, viene garantito a ENISA un mandato permanente, nel cui perimetro sono previsti compiti di consulenza tecnica, così come di supporto alla gestione operativa degli incidenti informatici da parte degli Stati membri.
Un secondo punto di attenzione contenuto nel *Cybersecurity Act* riguarda l'introduzione di un quadro complessivo di regole che disciplinano gli schemi europei di certificazione della sicurezza informatica senza definire, di per sé, schemi di certificazione direttamente operativi; al contrario viene creato un "framework" di base su cui istituire schemi europei per la certificazione. Sono previsti tre possibili livelli di certificazione di *affidabilità* relativamente alla cybersecurity: *livello base, sostanziale ed elevato*. Il livello di affidabilità è commisurato al rischio associato al previsto uso del prodotto, servizio o processo ICT, in termini di probabilità e impatto di un incidente.
Per i prodotti, servizi e processi ICT con livello di *rischio elevato* la certificazione può essere rilasciata solo dall'Autorità nazionale di cybersecurity, oppure, nei casi seguenti, da un organismo di valutazione della conformità:

a) previa approvazione dell'Autorità nazionale di certificazione della cybersecurity per ogni singolo certificato europeo di cybersecurity rilasciato da un organismo di valutazione della conformità; o
b) sulla base di una delega generale del compito di rilasciare tali certificati europei di cybersecurity a un organismo di valutazione della conformità da parte dell'Autorità nazionale di certificazione della cybersecurity.

In Italia, l'architettura nazionale di cybersecurity viene definita nel DL 82/2021, che istituisce il Sistema nazionale di sicurezza cibernetica e l'Agenzia per la Cybersicurezza Nazionale (ACN). All'ACN è attribuita, tra l'altro, la funzione di Autorità nazionale di certificazione della cybersecurity (*National Cybersecurity Certification Authority - NCCA*) e quindi di tutte le funzioni in materia di certificazione di sicurezza cibernetica, ivi comprese quelle relative al Perimetro di Sicurezza Nazionale Cibernetica (PSNC)[3].

---

[2] *European Union Agency for Cybersecurity (ENISA) è un centro di competenze in materia di sicurezza informatica istituito, nell'attuale configurazione, con il Regolamento UE 2019/881 (EU Cybersecurity Act). L'Agenzia Europea ha la missione di aiutare l'UE e i Paesi membri a essere meglio attrezzati e preparati nel prevenire, rilevare e reagire ai problemi di sicurezza dell'informazione. Contribuisce alla politica dell'UE in materia di sicurezza nel settore informatico, per migliorare l'affidabilità dei prodotti, dei servizi e dei processi ICT con programmi di certificazione della cybersicurezza.*

[3] *La normativa nazionale (DL 105/2019) sul Perimetro di Sicurezza Nazione Cibernetica (PSNC) cerca di mettere in opera, a livello italiano, tutte le prescrizioni e le disposizioni imposte dagli attuali Regolamenti europei in tema di cybersecurity, in particolar modo dalla Direttiva NIS e dal Cybersecurity Act. Con atti normativi successivi si è intervenuto a più riprese sul PSNC, in particolare:*
• con il DPCM 131/2020 (DPCM I) sono state definite le modalità e i criteri procedurali di individuazione dei soggetti pubblici e privati inclusi nel PSNC;
• con il DPCM 81/2021 (DPCM II) sono state specificate le modalità e il contenuto delle comunicazioni degli incidenti, da parte dei soggetti appartenenti al PSNC ed elencate una serie di misure di sicurezza che il soggetto del PSNC deve adottare e i relativi tempi di adozione per i beni ICT di propria pertinenza, inseriti in appositi elenchi;
• con il DPCM 15 giugno 2021 (DPCM III) sono state definite le tipologie di beni e servizi ICT che devono essere sottoposte a procedure di verifica e ispezione previste dal DPR 54/2021.

Successivamente, con il D.Lgs. 123/2022 viene adeguato l'ordinamento nazionale alle disposizioni contenute nel titolo III "Quadro di certificazione della cybersecurity" del Regolamento UE 2019/881.
In particolare viene confermato il ruolo dell'ACN in qualità di Autorità nazionale di certificazione della cybersecurity che svolge attività di vigilanza del mercato e rilascio di alcune tipologie di certificati europei di cybersecurity.
L'ACN vigilerà dunque sulla corretta applicazione delle regole previste dai sistemi europei di certificazione della cybersecurity da parte di: fornitori e fabbricanti di prodotti ICT (tecnologie dell'informazione e comunicazione), emittenti di dichiarazioni UE di conformità, titolari di certificati europei e organismi di valutazione della conformità.
Parallelamente, l'ACN, sulla base di un'apposita convenzione, supporterà attivamente l'Ente Unico nazionale di accreditamento (Accredia) nel monitoraggio e nella vigilanza delle attività degli organismi di valutazione della conformità da essa accreditati.
Nel dettaglio, l'ACN è direttamente competente al rilascio di certificazioni con livello di affidabilità elevato e, nello svolgimento di questo compito, si avvale dell'Organismo di Certificazione della Sicurezza Informatica (OCSI). Il rilascio potrà altresì avvenire a opera di un organismo di valutazione della conformità che agisca sulla base di una delega generale dell'ACN, oppure previa approvazione dell'ACN per ogni certificato rilasciato.
Le certificazioni con livello di affidabilità di base o sostanziale potranno essere rilasciate anche da organismi di valutazione accreditati ai sensi del Regolamento CE 765/2008. In tal caso, l'ACN parteciperà con propri rappresentanti alle deliberazioni sull'accreditamento degli organismi.
Accredia, nello svolgimento delle funzioni assegnatele dal Regolamento UE 2019/881, comunicherà all'ACN e all'ufficio unico di collegamento designato per l'Italia (Ministero dello Sviluppo Economico) ogni aggiornamento in merito agli organismi di valutazione accreditati (nuovi accreditamenti, revoche, sospensioni e le limitazioni del certificato di accreditamento).
L'Agenzia, inoltre, aggiornerà e renderà pubblici due elenchi di esperti e di laboratori di prova da essa abilitati a operare a supporto delle attività di vigilanza e rilascio dei certificati in capo all'Agenzia. Gli esperti e i laboratori di prova inseriti nell'elenco dei soggetti abilitati non potranno effettuare attività di valutazione per l'emissione di certificati con livello di affidabilità sostanziale o di base in ambito nazionale, né potranno essere accreditati come organismi di valutazione della conformità per il rilascio di tali certificati.
È disposto inoltre che, in assenza di un sistema europeo di certificazione, l'ACN potrà introdurre sistemi nazionali di certificazione per prodotti ICT, servizi ICT o processi ICT, previa consultazione dei portatori di interesse. Si ricorda che, al fine di evitare la frammentazione del mercato interno dei sistemi di certificazione, gli Stati membri dovranno informare la Commissione e il gruppo europeo per la certificazione della cybersecurity (ECCG) di ogni intenzione di elaborare nuovi sistemi nazionali di certificazione della cybersecurity.
Sempre in tema di certificazione per la cybersecurity, la Strategia Nazionale di Cybersicurezza 2022-2026 emanata a maggio 2022 dall'ACN promuove lo sviluppo di un quadro omogeneo e coerente degli standard europei per la cybersecurity. La Strategia individua dunque tre obiettivi fondamentali da perseguire: *protezione, risposta e sviluppo*. In particolare, nell'ambito dell'obiettivo 1 della Strategia (protezione degli asset strategici nazionali) viene ritenuto indispensabile il potenziamento delle capacità del Centro di Valutazione e Certificazione Nazionale (CVCN) dell'ACN e, negli ambiti di competenza, dei Centri di Valutazione (CV) del Ministero dell'Interno e della Difesa, nonché l'integrazione con una rete di Laboratori di Prova Accreditati.

La Strategia rafforza la necessità di definire un quadro giuridico nazionale aggiornato e coerente in materia di cybersecurity. In tale contesto, assumono rilevanza:

- il supporto allo sviluppo di schemi di certificazione e standard europei e internazionali in materia di cybersecurity;

- la promozione dell'utilizzo di schemi di certificazione europea in materia di cybersecurity, da parte delle imprese italiane specializzate, al fine di conseguire un vantaggio competitivo sul mercato.

I servizi accreditati per la cybersecurity

Il concreto rischio di compromissione dei sistemi informativi e presidi tecnologici, a cui si accompagna la possibile violazione di dati personali è in continua crescita. Nel 2021 gli attacchi informatici nel mondo sono aumentati del 10% rispetto all'anno precedente[4]. Le nuove modalità di attacco dimostrano che i cyber criminali sono sempre più sofisticati e in grado di fare rete con la criminalità organizzata. In questo quadro è importante impostare un'azione di preparazione agli attacchi, ma anche di capacità di rilevamento, contenimento e risposta. L'azione di sistema deve tendere a migliorare la postura di sicurezza globale, ma questo necessariamente passa attraverso un intervento che coinvolga i diversi comparti della società e del mondo produttivo.
Gli standard tecnici, assieme alle norme di carattere nazionale e comunitario, assumono un ruolo centrale. In particolare, la conformità rispetto a standard tecnici e norme significa capacità di definizione e di pianificazione delle strategie di cybersecurity. Significa anche capacità di monitoraggio delle azioni incardinate nella strategia adottata e, in ultimo, significa capacità di poter dimostrare, attraverso riferimenti obiettivi, la maturità delle proprie strategie di fronte a terzi. Quest'ultimo aspetto si fonda su due pilastri, tra di loro saldamente connessi: la valutazione della conformità alle norme tecniche e l'accreditamento. Quest'ultimo, in particolare, garantisce la sussistenza di profili di imparzialità, competenza e indipendenza degli organismi che rilasciano il servizio di valutazione della conformità. I servizi accreditati (certificazioni, ispezioni e verifiche svolti dagli organismi e dai laboratori accreditati) offrono garanzie sulla qualità e sulla sicurezza dei prodotti e dei servizi acquistati. Il beneficio apportato è significativo in una varietà di ambiti, ma diventa cruciale in un ambito sensibile quale quello della cybersecurity. Offrono garanzie sul rispetto di requisiti di sicurezza fondamentali, come la tutela della privacy e la protezione dell'erogazione dei servizi essenziali dalla minaccia cyber. Fin dal 2002, Accredia opera sia nell'ambito della sicurezza delle informazioni sia nell'ambito della cybersecurity.
Il coinvolgimento dell'Ente di accreditamento nell'ambito della cybersecurity è ampio e riguarda diverse competenze tecniche. Tra le altre, le principali sono:

- i Sistemi di Gestione per la Sicurezza delle Informazioni e la cybersecurity (ISMS);

- le competenze dei Professionisti operanti nell'ambito della sicurezza delle informazioni e della cybersecurity, inclusa la figura del Data Protection Officer (DPO) e dell'Auditor GDPR, oltre che la figura dell'Auditor di ISMS;

[4] *https://clusit.it/rapporto-clusit/*

- le certificazioni di prodotto, processo e servizio, come, ad esempio, quelle relative al sistema SPID e ai Regolamenti europei eIDAS e GDPR;

- le attività ispettive condotte a vari livelli, come ad esempio le ispezioni su impianti e strutture;

- i Laboratori di Prova, con riferimento ai processi di *Vulnerability Assessment* e a quelli di *Penetration Testing*.

Anche nel dominio della privacy e della tutela dei dati personali i servizi accreditati contribuiscono all'efficace realizzazione degli obiettivi definiti dal Regolamento europeo 2016/679, noto come *General Data Protection Regulation* (GDPR), il quadro normativo di riferimento in quest'ambito. Il Regolamento disciplina il diritto alla protezione dei dati personali, sancendo al contempo il principio della libera circolazione dei dati all'interno dell'Unione europea.
Il Regolamento prevede l'istituzione di "meccanismi di certificazione della protezione dei dati nonché di sigilli e marchi di protezione dei dati allo scopo di dimostrare la conformità al presente Regolamento dei trattamenti effettuati dai titolari del trattamento e dai responsabili del trattamento", senza pregiudicarne la responsabilità né far venire meno i compiti e i poteri delle Autorità di controllo nei loro confronti. Il Regolamento prevede che le certificazioni dovranno essere rilasciate da organismi accreditati ai sensi del Regolamento CE 765/2008 o dall'Autorità di controllo competente. In Italia, il Garante per la Protezione dei Dati Personali ha deciso di affidare ad Accredia l'accreditamento degli schemi di certificazione, che dovranno essere approvati dal Garante stesso.
Viene introdotta la figura del Data Protection Officer (DPO)[5] a supporto delle organizzazioni pubbliche, con il fine di informare e fornire consulenza al titolare del trattamento[6] o al responsabile del trattamento[7], nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal GDPR. Si tratta di un professionista con elevata conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti attribuitigli dalla norma. Il mondo della normazione tecnica ha disciplinato tale figura professionale attraverso la norma volontaria UNI 11697 e la Prassi di Riferimento UNI/Pdr 66:2019. L'importanza legata alle funzioni ricoperte dal DPO, la necessità di avere garanzie circa l'efficacia della propria azione e, non ultima, l'importanza di qualificare le proprie competenze rispetto al mercato ha portato, nonostante la volontarietà dello schema, ben 15 organismi di certificazione ad accreditarsi ai sensi della norma ISO/IEC 17024 e 687 professionisti a certificare le proprie competenze.

---

[5] In Italia è stata redatta una norma tecnica volontaria con la quale vengono stabiliti i requisiti relativi ai professionisti che opereranno nell'ambito del trattamento e della protezione dei dati personali. È bene ricordare che, pur non avendo formalmente riconosciuto queste certificazioni, il Garante per la Protezione dei Dati Personali ha preso parte alle fasi di sviluppo della UNI 11697:2017, partecipando al tavolo di lavoro per la redazione della norma. A oggi, la certificazione UNI 11697:2017, ottenuta da un organismo accreditato secondo la ISO/IEC 17024, è ritenuta una presunzione di competenza dei membri del gruppo di verifica quando certificano in ambito privacy.
[6] È la persona fisica o giuridica, l'Autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali.o.
[7] Definito come la persona fisica o giuridica, l'Autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.

Di seguito, in tabella 1, sono riportati i principali schemi di valutazione di conformità accreditati in ambito cybersecurity per i quali sono stati già rilasciati i relativi certificati di accreditamento.

Tabella 1 - Cybersecurity - schemi di valutazione di conformità accreditati - agg 13/10/2022

Norma di accreditamento	Norma di certificazione	Descrizione	Nr. accreditamenti	Nr. Certificazioni
ISO/IEC 17021-1	ISO/IEC 20001-1	Sistemi di gestione per i servizi informatici	9 organismi di certificazione	327 aziende certificate
ISO/IEC 17021-1	UNI ISO 27001	Sistemi di gestione per la sicurezza delle informazioni	20 organismi di certificazione	3.474 aziende certificate
ISO/IEC 17021-1	UNI EN ISO 22301	Sistemi di gestione della continuità aziendale	9 organismi di certificazione	222 aziende certificate
ISO/IEC 17025		Vulnerability Assessment	5 laboratori di prova	
ISO/IEC 17024	UNI 11697:2017 UNI PdR 66:2019 ECF PRIVACY	Responsabile della protezione dei dati	15 organismi di certificazione	687 persone certificate
ISO/IEC 17024	UNI 11506 Norme UNI 11621-x (Multiparte)	Figure dei Professionisti ICT (WEB, Security, Operations)	7 organismi di certificazione	250 persone certificate
ISO/IEC 17020	Cyber Security Framework Nazionale – CSF 2.0 Febbraio 2019	Ispezione di Tipo A/C	2 organismi di ispezione	
ISO/IEC 17065	ISDP©10003:2015	Certificazione dei processi per la tutela delle persone fisiche con riguardo al trattamento dei dati personali – Reg. UE 679/2016	2 organismi di certificazione	16 aziende certificate
ISO/IEC 17065	UNI/PdR 43	Linee guida per la gestione dei dati personali in ambito ICT secondo il Regolamento UE 679/2016 (GDPR)	2 organismi di certificazione	12 aziende certificate
ISO/IEC 17065	Serie IEC 61508 Serie IEC 61511 IEC 62061 Serie ISO 26262	Sicurezza Funzionale	3 organismi di certificazione 1 organismo di ispezione	
ISO/IEC 17065	Serie IEC 62443	Sicurezza dei sistemi OT (Operational Technology)	2 organismi di certificazione	
ISO/IEC 17065 ETSI 319 403	Regolamento eIDAS Norme serie ETSI 319 401 Norme dedicate ai Servizi dei TSP	Conformità al Regolamento eIDAS e Servizi dei TSP	7 organismi di certificazione	
ISO/IEC 17065	Specifica Tecnica [Check List] di AgID	Servizi SPID	4 organismi di certificazione	

Lo studio dei benefici derivanti dall'utilizzo dei servizi accreditati

È possibile fornire una misura concreta del beneficio portato dall'utilizzo dei servizi accreditati per la cybersecurity?
Per rispondere a questa domanda, sono state adottate due metodologie complementari: una prima, basata sull'analisi di casi di studio selezionati che ha condotto alla definizione di una serie di indicazioni qualitative legate al beneficio derivante dall'ottenimento e mantenimento di una certificazione accreditata per la norma UNI CEI EN ISO/IEC 27001. La seconda metodologia si è basata su attività di analisi delle vulnerabilità dei servizi web esposti da un vasto campione di organizzazioni, con la messa in relazione degli esiti di tale analisi rispetto al possesso (o meno) di una certificazione accreditata per la UNI CEI EN ISO/IEC 27001. Questa seconda metodologia di analisi ha consentito di ottenere indicatori di carattere quantitativo circa il livello di esposizione al rischio delle aziende certificate. Un'attività di questo tipo è in grado di fornire indizi molto chiari circa la postura di sicurezza dell'organizzazione, essendo proprio i servizi web quelli maggiormente presi di mira dagli attaccanti per assicurarsi un punto di ingresso nel perimetro dell'organizzazione. L'analisi dei casi di studio è partita dall'individuazione delle aziende da intervistare. La selezione si è basata su specifici fattori che tenessero conto della dimensione, natura, mercato di riferimento ed età della certificazione. Sulla base di questi fattori, è stata considerata una lista delle aziende italiane con certificazione UNI CEI EN ISO/IEC 27001 da cui sono stati selezionati i seguenti casi di studio:

- *Gruppo BCC Iccrea* - È il maggiore gruppo bancario cooperativo italiano, l'unico gruppo bancario nazionale a capitale interamente italiano e il quarto gruppo bancario in Italia per attivi. Il Gruppo BCC Iccrea è costituito[8] da 120 Banche di Credito Cooperativo presenti in oltre 1.700 comuni italiani con quasi 2.500 sportelli, e da altre società bancarie, finanziarie e strumentali controllate dalla Capogruppo, BCC Banca Iccrea, che eroga servizi in ambito finanza, crediti istituzionali, amministrazione titoli e sistemi di pagamento. Il Gruppo conta più di 3 milioni di clienti, circa 845.000 Soci e oltre 22.000 dipendenti.

- *Poste Italiane* - Il gruppo, con i suoi 160 anni di storia, costituisce la più grande rete di distribuzione di servizi in Italia, attiva nei settori della logistica, nella consegna di corrispondenza e pacchi, nei servizi finanziari e assicurativi, nei sistemi di pagamento e nella telefonia.

- *Atac* - L'azienda per la mobilità del Comune di Roma è il primo operatore della mobilità urbana in Italia e una delle più grandi realtà di gestione del Trasporto Pubblico Locale in Europa. Oggi Atac conta su più di 10.000 unità di personale con ruoli e professioni estremamente diversificati.

- *Notartel* - La società del Consiglio Nazionale del Notariato e della Cassa Nazionale che offre servizi IT ai notai italiani da oltre vent'anni. Da diversi anni gestisce l'emissione di Firma Digitale e smart card e il servizio di Posta Elettronica Certificata dei notai italiani, oltre che essere l'Ente Conservatore per conto del Consiglio Nazionale del Notariato.

L'analisi dei casi di studio ha consentito di tracciare alcuni elementi generali legati alla certificazione dell'ISMS. Un primo punto rilevante è che difficilmente le motivazioni che sottendono la decisione di certificare il proprio ISMS rappresenteranno nel tempo l'unico ritorno degli investimenti fatti.

[8] *Dati al 30 giugno 2022.*

Tutte le esperienze raccolte con i casi di studio hanno permesso di capire come solo con il tempo le organizzazioni certificate riescano a comprendere in modo approfondito quanto il percorso seguito abbia cambiato profondamente la loro organizzazione, con un miglioramento tangibile in molti contesti, non necessariamente limitati alla migliore gestione del rischio cibernetico.
Un secondo aspetto è il fatto che la certificazione di un ISMS è un elemento facilitatore per la conformità rispetto ai numerosi regolamenti che, in diversi settori, impongono requisiti legati alla cybersecurity. L'approccio *risk-based* rappresenta, da un lato, uno dei valori aggiunti più importanti acquisiti con l'adozione di questo tipo di ISMS, ma anche uno dei punti critici nella fase di adeguamento e successivamente di miglioramento e mantenimento della certificazione. Le attività necessarie in questo senso sono tante, impegnative e, spesso, richiedono di rivoluzionare il modo di pensare di una organizzazione. Il costo di tutto questo, in termini anche di risorse umane, può essere importante e non necessariamente alla portata degli attori di dimensioni più piccole o che devono operare in mercati altamente competitivi.
Una volta superati questi ostacoli, un ISMS può contribuire positivamente alla vita dell'organizzazione attraverso una omogeneizzazione dei processi di monitoraggio e miglioramento degli stessi, di valutazione delle prestazioni e di auditing indipendenti che permettono all'organizzazione di gestire in modo ragionato e coerente criticità, incidenti e futuri adeguamenti. Gli standard per la gestione della sicurezza e i relativi processi di certificazione rappresentano un vero e proprio *driver* per la crescita culturale delle organizzazioni che li adottano. La cultura della sicurezza e tutto ciò che ne deriva richiedono anni per svilupparsi. Questo tipo di investimento ha un ritorno a lungo termine, che garantisce benefici duraturi, che diventano parte integrante dell'organizzazione.
La seconda metodologia di analisi dei potenziali benefici derivanti dall'utilizzo dei servizi accreditati si basa su uno studio tecnico su due popolazioni di organizzazioni private e pubbliche italiane: una dotata di certificazione per la sicurezza UNI CEI EN ISO/IEC 27001 e una dotata di certificazione per la qualità UNI EN ISO 9001:2015. In particolare, attraverso una campagna di *Vulnerability Assessment* (non invasiva) dei servizi web esposti al pubblico dalle stesse organizzazioni, è stato possibile valutare:

- il posizionamento dei software utilizzati per tali servizi rispetto alle gravi vulnerabilità note incluse nei database nazionali e internazionali (ad es. il CVE database);
- il corretto utilizzo del protocollo HTTPS;
- i livelli di aggiornamento e sicurezza dei Content Management System (CMS).

Ai fini dell'analisi sono state considerate tutte le organizzazioni pubbliche e private aventi sede legale sul territorio italiano, presenti nella banca dati di Accredia e in attività alla data di estrazione (marzo 2022). Tali organizzazioni sono state quindi suddivise in due diverse popolazioni[9], costituite da:

1. le organizzazioni provviste della certificazione di sicurezza UNI CEI EN ISO/IEC 27001;
2. le organizzazioni provviste della certificazione di qualità UNI EN ISO 9001.

[9] *Sono state escluse le organizzazioni che possiedono entrambe le certificazioni per evitare sovrapposizioni tra le due popolazioni.*

Sono state estratte 100 organizzazioni, 50 dal primo gruppo e 50 dal secondo, utilizzando la tecnica di "campionamento non probabilistico di convenienza" tenendo conto della dimensione aziendale e del settore di attività di appartenenza.
In generale le organizzazioni certificate UNI CEI EN ISO/IEC 27001 sono meno suscettibili a gravi vulnerabilità di sicurezza. L'attività di analisi sulle vulnerabilità identificate tramite le fonti OSINT[10] ha permesso di individuare 1.207 vulnerabilità CVE sui 100 servizi web oggetto di analisi, di cui 683 (57%) nel campione di organizzazioni certificate UNI EN ISO 9001 e 524 (43%) nel campione certificato UNI CEI EN ISO/IEC 27001.
L'attività di analisi sull'utilizzo del protocollo HTTPS ha evidenziato come le organizzazioni UNI CEI EN ISO/IEC 27001 abbiano un alto grado di sicurezza nell'utilizzo del protocollo; il 50% del campione analizzato ha ottenuto valutazioni A e A+ (il massimo grado di sicurezza). Il 42% invece ha raggiunto il grado B, superando pienamente la sufficienza.
Per quanto riguarda, invece, le organizzazioni certificate UNI EN ISO 9001 solo il 37% riesce a raggiungere il massimo grado di configurazione di sicurezza (A, A+), mentre il 50% dei servizi si attesta sul grado di sicurezza B.
Infine l'attività di analisi sui servizi web del campione ha permesso di individuare la presenza di diverse tecnologie di Content Management System (CMS). Nel 62,7% dei siti web analizzati è stato riscontrato l'utilizzo di un CMS appartenente a 8 tecnologie differenti.
L'attività di analisi è proseguita andando a determinare, per ogni CMS, il numero di versione, con l'obiettivo di valutare il livello di aggiornamento dei CMS, che sono spesso oggetto di vulnerabilità di sicurezza ad alto impatto.
Il 24% delle organizzazioni UNI CEI EN ISO/IEC 27001 risulta avere una versione aggiornata del proprio CMS, a differenza della controparte certificata UNI EN ISO 9001 che si attesta al 18%.
Le attività di analisi quantitativa – pur non rappresentando una valutazione esaustiva dello stato di sicurezza di un'organizzazione – hanno confermato una migliore postura di sicurezza delle organizzazioni con una certificazione accreditata per la UNI CEI EN ISO/IEC 27001.

Prospettive future sul contributo dei servizi accreditati per la cybersecurity

Ai servizi accreditati di cybersecurity è riconosciuto un ruolo centrale nel costruire relazioni di "fiducia" tra produttori e consumatori di prodotti e servizi digitali. Tale ruolo è destinato a crescere alla luce delle iniziative nazionali e comunitarie tese a rafforzare le difese e la resilienza dei servizi digitali e, più in generale, delle funzioni essenziali dello Stato quali, ad esempio, la Strategia Nazionale di Cybersicurezza, pubblicata dall'ACN, e il *Cybersecurity Act*.
La Strategia Nazionale di Cybersecurity è posta in continuità con i provvedimenti normativi di recepimento della Direttiva NIS e di quelli correlati, che hanno portato alla creazione del "Perimetro di Sicurezza Nazionale Cibernetica". Le organizzazioni che operano nel suddetto "perimetro" dovranno far valutare alcune categorie dei propri asset dal Centro di Valutazione e Certificazione Nazionale (CVCN) dell'ACN e dovranno seguire le prescrizioni di sicurezza fornite dall'ACN.

---

[10] *Le tecniche di Open Source INTelligence (OSINT) sono volte a sfruttare tutte le informazioni pubbliche disponibili e reperibili, come descritto nel set di controlli WSTG-INFO "Information Gathering".*

Questo servizio si realizzerà attraverso un processo di accreditamento che ricadrà sotto le previsioni del Regolamento CE 765/2008, tramite la collaborazione operativa tra l'ACN, Accredia e i laboratori oggetto di accreditamento da parte della stessa Accredia.
Oltre alle certificazioni di prodotto, di particolare rilevanza è l'area delle certificazioni degli ISMS, ma anche della erogazione dei servizi ICT di tipo fiduciario.
Senza questa componente sistemica, le sole certificazioni di prodotto rischiano di non avere l'effetto desiderato.
I 20 organismi di certificazione accreditati da Accredia per i sistemi di gestione per la sicurezza delle informazioni (UNI CEI EN ISO/IEC 27001) svolgono il monitoraggio (certificazione iniziale, sorveglianze e rinnovi) di circa 3.500 aziende che, insieme ai 5 laboratori e ai *Trust Service Providers* in ambito SPID ed eIDAS, assommano a circa 4.300 soggetti.
La creazione del *know-how* dei professionisti impiegati nelle attività di accreditamento a garanzia dei servizi di valutazione di conformità forniti da tali soggetti non è un processo breve, né semplice. Basti considerare che i professionisti in possesso di certificazione professionale per gli audit nell'ambito della sicurezza delle informazioni non superano i 40 in tutto il Paese.
L'allargamento del perimetro di sicurezza, che verrà verosimilmente introdotto con la cosiddetta Direttiva NIS2, e che porterebbe il numero delle organizzazioni sotto il monitoraggio ACN a diverse migliaia di unità, sarà difficilmente gestibile nel breve periodo. E allora un dialogo e una stretta collaborazione tra l'ACN e Accredia non è solo auspicabile, ma necessaria. E questa è la direzione in cui si muovono in maniera proattiva i due Enti, con la sigla della Convenzione che regola le modalità di fruizione da parte dell'ACN, dei servizi di valutazione della conformità da parte di Accredia e dà applicazione al D.Lgs. 123/2022.
Per quanto il contesto sia particolarmente favorevole per un più ampio utilizzo dei servizi accreditati di cybersecurity, va osservato come gli attuali schemi di certificazione non sempre soddisfino le esigenze di importanti settori del mercato.
La messa a punto di schemi di certificazione capaci di offrire un livello di sicurezza adeguato a contesti operativi caratterizzati da un livello di rischio non elevato, senza incorrere in tempi e costi particolarmente gravosi, detti *schemi di certificazione leggera (lightweight certification)*, consentirebbe di allargare significativamente la platea dei possibili fruitori, con un notevole beneficio collettivo.
Per cogliere appieno le opportunità offerte dalla crescente attenzione sui servizi accreditati di cybersecurity è fondamentale che gli schemi di certificazione possano evolvere nelle direzioni richieste dal mercato. In particolare:

- il modello DevOps che combina le fasi di sviluppo (*Development* in inglese) e di messa in operazione (*Operations* in inglese) del software assicurando che le nuove funzionalità introdotte in fase di sviluppo vengano messe in operazione in tempi rapidissimi. Tale modello apre infatti scenari interessanti per la certificazione dei prodotti software. In particolare, la possibilità di inserire controlli automatici di sicurezza nelle varie fasi del ciclo di vita dell'applicazione consentirebbe di generare automaticamente la documentazione necessaria per la certificazione non solo della versione iniziale del prodotto, ma di tutte le versioni che verranno successivamente rilasciate. Verrebbero resi più efficienti, sia dal punto di vista dei tempi sia dei costi, gli schemi di certificazione di cybersecurity *leggeri*.

- Nati in ambito militare, i *Cyber-Range* sono piattaforme informatiche che, grazie alle tecnologie della virtualizzazione, supportano la simulazione di attacchi cyber in scenari ICT di elevato realismo. I *Cyber-Range*, supportano l'esecuzione di attacchi sofisticati e su larga scala offrendo un'inedita opportunità per la creazione di schemi di certificazione di nuova generazione, finalizzati alla valutazione delle competenze del personale, dei prodotti di cybersecurity e dei processi aziendali.

In ultimo, un ulteriore elemento di analisi del potenziale coinvolgimento futuro dei servizi accreditati per la cybersecurity riguarda la certificazione delle competenze professionali. Si tratta di un aspetto già al centro della produzione normativa europea e nazionale. L'attenzione nasce dall'esigenza di personale qualificato su competenze specialistiche e in continua evoluzione. Infatti, nonostante nel panorama delle certificazioni professionali in ambito ICT, siano già oggi disponibili nel mercato, tra le altre, le certificazioni previste dalla norma UNI 11506 e dalle norme cosiddette "multiparte", della serie UNI 11621, va notata una carenza di competenze in materia di cybersecurity. In questo contesto sono state intraprese azioni non solo per aumentare la forza lavoro nel campo della cybersecurity, ma anche per aumentare la qualità dei candidati e dotarli delle competenze più richieste dal settore. Esempi sono i programmi CyberChallenge.it, OlyCyber.it e CyberTrials promossi, nel contesto italiano, dal Cybersecurity National Lab del CINI. A livello normativo lo *European Cybersecurity Skills Framework* (ECSF) mira a creare una comprensione comune dei ruoli, delle competenze, delle abilità e delle conoscenze utilizzate da e per gli individui, i datori di lavoro e i fornitori di formazione in tutti gli Stati membri dell'UE, al fine di affrontare la carenza di competenze in materia di sicurezza informatica. Inoltre, nelle intenzioni del Legislatore, contribuirà a facilitare ulteriormente il riconoscimento delle competenze in materia di cybersecurity e a sostenere la progettazione di programmi di formazione in materia di cybersecurity per lo sviluppo delle competenze e della carriera. Obiettivi simili sono stati inseriti anche nel rinnovato *Digital Education Action Plan* (2021-2027)[11].
In Italia, la Strategia Nazionale di Cybersicurezza promuove la cultura sulla sicurezza cibernetica. L'obiettivo è favorire una conoscenza diffusa sui rischi connessi all'utilizzo di strumenti digitali e diffondere specifiche competenze in materia di cybersecurity. In particolare si prevede, al fine di garantire l'efficacia dei percorsi formativi, lo sviluppo di un sistema nazionale di certificazione dell'apprendimento e dell'acquisizione di specifiche professionalità, non solo tecniche, sia a livello di istruzione secondaria di secondo grado, sia a livello universitario e professionale. L'ACN dovrà mantenere una lista dei percorsi di formazione, approvati dalla stessa Agenzia, al termine dei quali verrà rilasciata la relativa certificazione.

[11] *https://education.ec.europa.eu/focus-topics/digital-education/digital-education-action-plan*

Osservatorio
ACCREDIA

Via Guglielmo Saliceto, 7/9
00161 Roma

Tel. +39 06 844099.1
Fax. +39 06 8841199

info@accredia.it
www.accredia.it

ACCREDIA
L'ENTE ITALIANO DI ACCREDITAMENTO