Osservatorio ACCREDIA

1 | 2022

Cybersecurity e protezione dei dati: il ruolo della certificazione accreditata

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

Lo studio è stato 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

Abstract

La cybersecurity ha assunto un ruolo di primo piano nell'agenda di Governi, Istituzioni, aziende, rientrando tra le principali priorità dei Paesi dell'Unione europea, in accordo alle quali devono essere definite le strategie di sviluppo, attraverso azioni di coordinamento normativo, tecnico e operativo. Si tratta di un ambito in cui il grado di strutturazione delle azioni da compiere gioca un ruolo determinante, ai fini della loro efficacia. Strutturare la cybersecurity significa per prima cosa dotare ogni dominio di azione di precisi fondamenti normativi e regolatori, che rappresentano la guida all'interno dei quali gli interventi possono o devono essere assunti. Le norme non delineano solo principi e linee programmatiche, ma definiscono vere e proprie strategie, che vengono poi declinate, attraverso provvedimenti che introducono *norme tecniche (standard)*, in un'accezione operativa. In tutto questo, gli standard, assieme alle norme di carattere nazionale ed europeo, assumono un ruolo centrale. Sebbene il panorama degli standard di sicurezza sia vastissimo – come del resto sconfinata è la materia – il binomio norme e standard permette di raggiungere un quadro organico e ordinato, offrendo punti di riferimento precisi e percorsi di intervento codificati e verificabili.

Di conseguenza, per una organizzazione, sia essa pubblica o privata, la conformità a standard e norme non significa soltanto tutela rispetto a sanzioni o responsabilità, ma anche capacità di definizione e di pianificazione in modo corretto e completo delle strategie di cybersecurity e delle azioni conseguenti, capacità di monitorare l'adozione delle strategie in ogni fase, misurandone il grado di attuazione e la loro efficacia, nonché capacità di poter dimostrare, attraverso riferimenti obiettivi, la maturità delle proprie strategie di fronte a terzi. Quest'ultimo aspetto si fonda su due pilastri saldamente connessi: la certificazione e l'accreditamento.

La ricerca condotta, attraverso il presente rapporto, mostra quanto certificazione e accreditamento sviluppino una funzione portante nell'ambito della cybersecurity. Funzione che irrinunciabilmente deve assicurare affidabilità all'intero processo, a tutte le sue componenti, e con essa anche quel necessario grado di standardizzazione, misurabilità, interoperabilità, controllo e leggibilità delle strategie e tattiche adottate.

Riferendosi soprattutto al panorama nazionale ed europeo, il rapporto presenta lo stato dell'arte sulla normativa e sui regolamenti con duplice obiettivo di offrire un quadro di riferimento e di legare l'azione normativa e regolatoria con gli aspetti e i requisiti di certificazione che essa stessa disciplina. In questo ambito la Strategia Nazionale di Cybersicurezza 2022-2026 mira al potenziamento del Centro di Valutazione e Certificazione Nazionale (CVCN) dell'Agenzia per la Cybersicurezza Nazionale (ACN) e dei Centri di Valutazione (CV) del Ministero dell'Interno e della Difesa, nonché all'integrazione con una rete di *laboratori di prova accreditati*.

In questo rapporto vengono quindi introdotte le nozioni di certificazione e accreditamento attraverso l'analisi delle certificazioni rilevanti nel dominio della cybersecurity e dei relativi processi di accreditamento. L'analisi è condotta a largo spettro e include, tra le altre cose, il dominio della tutela e della protezione dei dati e il dominio delle identità e firme elettroniche, nel quadro di riferimento europeo definito dai Regolamenti europei GDPR ed eIDAS. Tali esempi mostrano con chiarezza i benefici derivanti dai processi di certificazione e accreditamento ed evidenziano il ruolo di ispezione e di vigilanza che il processo di accreditamento attribuisce agli Enti preposti. Viene quindi affrontato il tema della relazione che esiste tra cybersecurity, certificazione e accreditamento provando a dare una risposta alla domanda: dal punto di vista disciplinare non vi è alcun dubbio circa gli effetti benefici della certificazione e dell'accreditamento nell'ambito della cybersecurity, ma è possibile identificare una metodologia, dapprima, e un insieme di indicatori qualitativi e/o quantitativi, successivamente, che possano fornire non solo prova di questo asserto, ma anche un modo per misurare il grado di questi benefici? Per rispondere a questa domanda, sono state proposte e adottate due metodologie complementari. La prima basata sulla definizione e somministrazione di un insieme di domande, opportunamente classificate, sottoposte a stakeholder selezionati in modo da offrire un quadro di indagine significativo e sulla conseguente analisi delle risposte raccolte. Gli indicatori ottenuti attraverso questa metodologia sono chiaramente di natura qualitativa.
La seconda metodologia si è invece 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 di cybersecurity (in particolare secondo la norma tecnica ISO/IEC 27001) e di ulteriori caratteristiche dell'organizzazione. L'analisi, riportata in maniera completamente anonima, offre indicatori di carattere quantitativo che hanno permesso di trarre conclusioni coerenti con le premesse e con l'analisi disciplinare della tematica.
Lo studio, oltre a offrire un punto di vista ampio e diversificato della certificazione e dell'accreditamento in ambito di cybersecurity e tutela dei dati personali, conferma il principio secondo il quale la certificazione e l'accreditamento rappresentano fattori abilitanti per la cybersecurity, esercitando quindi un ruolo determinante nell'attuale processo di trasformazione digitale della società.

Lo studio "Cybersecurity e protezione dei dati: il ruolo della certificazione accreditata" è stato realizzato dall'Osservatorio congiunto "Cybersecurity e Certificazione" costituito da Accredia e dal Cybersecurity National Lab del Consorzio Interuniversitario Nazionale per l'Informatica (CINI), con l'obiettivo di monitorare le evoluzioni tecnico-normative, rilevare e portare all'attenzione degli stakeholder nuovi problemi e opportunità, e promuovere la cultura della valutazione della conformità nella cybersecurity. Il CINI è costituito da 49 Università pubbliche italiane e promuove e coordina attività scientifiche, di ricerca e di trasferimento, sia di base sia applicative, nel campo dell'informatica, di concerto con le comunità scientifiche nazionali di riferimento. Il Cybersecurity National Lab è uno dei laboratori tematici del CINI, che coordina una rete di 59 Nodi interconnessi, presso le principali Università, Istituti di ricerca e Accademie Militari, impegnando più di 800 tra professori e ricercatori. **www.consorzio-cini.it**

Osservatorio ACCREDIA 1 2022

Cybersecurity e protezione dei dati: il ruolo della certificazione accreditata

1. Introduzione

La *cybersecurity*[1] ha assunto un ruolo di primo piano nell'agenda di Governi, Istituzioni, aziende, rientrando tra le principali priorità dei paesi dell'Unione europea, in accordo alle quali devono essere definite le strategie di sviluppo, attraverso azioni di coordinamento normativo, tecnico e operativo. Con lo sviluppo della società digitale e la pervasività dei servizi ICT, il tema della cybersecurity sta infatti assumendo sempre più un ruolo strategico e quindi un'opportunità per le imprese operanti nei settori dell'ICT, ma, d'altra parte, è diventato anche un problema da affrontare con estrema 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 i cui effetti possono essere devastanti, comportando l'interruzione di servizi di utilità pubblica, come la distribuzione di energia elettrica o di gas, i sistemi di telecomunicazioni, le infrastrutture di trasporto, ecc. La cybersecurity è diventato pertanto un problema complesso per il quale sono necessarie soluzioni efficaci e coordinate: nessun anello della catena della sicurezza deve essere trascurato, incluso l'utente finale che spesso è esso stesso, con il suo comportamento, fonte di vulnerabilità.

1.1 Contesto di riferimento

Famiglie, imprese e Pubbliche Amministrazioni sperimentano quotidianamente il crescente livello di rischio a cui sono esposte nelle attività eseguite con strumenti informatici e con il supporto di infrastrutture IT per la comunicazione dei dati.
Le operazioni svolte tramite sistemi IT, dalla trasmissione di dati all'utilizzo di supporti di elaborazione e memorizzazione esterni, ormai nella disponibilità di tutti grazie alla riduzione dei costi, sono esposti a un crescente livello di minaccia sul fronte della gestione della sicurezza delle informazioni. Quotidianamente abbiamo evidenza dei danni provocati da tali attacchi, sia a singoli utenti che a importanti infrastrutture produttive e di servizi. Si va dal blocco di sistemi IT privati o pubblici, all'esfiltrazione di informazioni personali (es. dati sanitari). Gli episodi di ostilità informatica emersi negli ultimi anni, sviluppati in maniera dolosa attraverso il cyberspazio, hanno portato alla luce l'esistenza di organizzazioni specializzate in azioni di criminalità informatica.

---

[1] *Nel documento, con il termine cybersecurity si intende il concetto definito dall'art. 1 del DL 82/2021: "l'Insieme delle attività necessarie per proteggere dalle minacce informatiche reti, sistemi informativi, servizi informatici e comunicazioni elettroniche, assicurandone la disponibilità, la confidenzialità e l'integrità, e garantendone altresì la resilienza".*

Questi attacchi sfruttano debolezze di vario tipo, dalla configurazione non corretta dei sistemi, ai mancati aggiornamenti software, e spesso sono perpetrati tramite software malevoli (i cosiddetti "malware") attentando alla riservatezza, integrità e disponibilità delle informazioni.
In più casi si è arrivati al danneggiamento irreversibile della stessa infrastruttura IT e di quella OT, vale a dire delle strutture fisiche industriali a questa collegate e da questa gestite. È questo il caso degli attacchi ai sistemi SCADA (Supervisory Control And Data Acquisition) e ICS (Industrial Control Systems) per la gestione dei processi industriali. Gli effetti sono stati equiparabili agli attacchi "cinetici" (quelli delle armi convenzionali) e quindi classificabili come veri atti di ostilità militare o paramilitare. Solo per fare alcuni esempi, si ha notizia certa di blocchi di centrali di produzione dell'energia (Iran 2010, tramite Stuxnet[2]; Ucraina 2015, tramite BlackEnergy[3]; UK 2017 National Health Services tramite WannaCry[4]; LazioCrea 2021 tramite un Ransomware[5]), con danni per decine di migliaia di cittadini e, talora, con gravi danneggiamenti degli stessi impianti. Sono stati registrati anche dei tentativi di avvelenamento dei sistemi di distribuzione idrica, tramite l'alterazione della clorazione dell'acqua potabile fatta prendendo possesso da remoto del sistema di controllo (cittadina di Oldsmar, in Florida, febbraio 2021[6]). L'approccio delle organizzazioni alla sicurezza delle informazioni non può essere delegato all'acquisto di strumenti hardware e software di difesa e protezione, ma richiede l'adozione di logiche sistemiche per la gestione di tutte le attività necessarie a mettere in sicurezza i propri processi gestionali e produttivi. L'approccio ritenuto più maturo ed efficace è quello della gestione secondo logiche iterative, tipiche dei sistemi di gestione basati sul cosiddetto "ciclo di Deming", noto anche con l'acronimo di PDCA (Plan, Do, Check and Act).
Ci si attende che i domini oggetto dell'applicazione dei cosiddetti ISMS (Information Security Management Systems) siano quello fisico (nel contesto reale dove operano le persone e vi è il cosiddetto hardware), quello logico (il contesto interconnesso e virtuale governato da software e algoritmi) e quello organizzativo (l'insieme delle regole di governance dell'organizzazione) per la tutela della riservatezza, integrità e disponibilità dei dati (e delle informazioni che se ne possono dedurre).
Infine, è da notare come gli attacchi informatici nel mondo hanno un trend sempre crescente: solo nel 2021 sono aumentati del 10% rispetto all'anno precedente[7]. Le nuove modalità di attacco dimostrano che i cyber criminali sono sempre più sofisticati e in grado di fare rete con la criminalità organizzata. Tra gli attacchi gravi di dominio pubblico, l'11% è riferibile ad attività di spionaggio e il 2% a campagne di Information Warfare. Nel 2021, sono stati registrati su scala globale 2.049 cyber attacchi "gravi", con una media di 171 incursioni al mese: il valore più elevato registrato finora. I cyber criminali hanno smesso di "pescare a strascico" e hanno bersagli sempre più definiti: al primo posto c'è l'obiettivo governativo/militare, con il 15% degli attacchi totali, in crescita del 36,4% rispetto all'anno precedente; segue il settore informatico, colpito nel 14% dei casi (+3,3% rispetto al 2020), gli obiettivi multipli (13%, in discesa dell'8%) e la sanità, che rappresenta, al pari, il 13% del totale degli obiettivi colpiti, in crescita del 24,8% rispetto ai dodici mesi precedenti. Segue l'istruzione, pari al 9% del totale, sostanzialmente stabile rispetto al 2020. Gli attacchi si sono verificati nel 45% dei casi nel continente americano (in leggero calo rispetto al 2020) mentre, in Europa, dove sono cresciuti, gli attacchi superano un quinto del totale (21%, contro il 16% dell'anno precedente).

---

[2] *https://arstechnica.com/tech-policy/2012/06/confirmed-us-israel-created-stuxnet-lost-control-of-it/*
[3] *https://www.reuters.com/article/us-ukraine-cybersecurity-sandworm-idUSKBN0UM00N20160108*
[4] *https://www.nao.org.uk/report/investigation-wannacry-cyber-attack-and-the-nhs/*
[5] *https://roma.repubblica.it/cronaca/2021/08/04/news/attacco_hacker_regione_rivendicazioni_errori-312887837/*
[6] *https://www.ilpost.it/2021/02/09/florida-acqua-avvelenata-liscivia-hacker/*
[7] *https://clusit.it/rapporto-clusit/*

Anche in Asia è in crescita il numero di attacchi arrivati al 12% rispetto al totale (dal 10% del 2020). Resta sostanzialmente invariata la situazione degli attacchi verso Oceania (2%) e Africa (1%). Anche la severità degli attacchi è in forte aumento rispetto all'anno precedente: il 79% degli attacchi rilevati ha avuto un impatto "elevato", contro il 50% dello scorso anno: in dettaglio, il 32% è stato caratterizzato da un impatto "critico" e il 47% "alto". A fronte di queste percentuali, sono diminuiti invece gli attacchi di impatto "medio" (-13%) e "basso" (-17%). L'aumento della gravità degli attacchi, inoltre, ha prodotto un effetto moltiplicatore sui danni, stimati nel 2021 in 6 trilioni di dollari, a fronte di 1 trilione di dollari valutato per il 2020.
L'analisi di queste dinamiche conferma come negli ultimi anni sia avvenuto un vero e proprio cambiamento epocale nei livelli globali di cyber-insicurezza, causato dall'evoluzione rapidissima degli attori di minaccia, delle modalità, della pervasività e dell'efficacia degli attacchi, al quale non è corrisposto un incremento sufficiente delle contromisure adottate dalle stesse organizzazioni.

1.2 La visione strutturata della cybersecurity

Il quadro sopra descritto evidenzia l'importanza e l'urgenza di un'azione di preparazione agli attacchi, ma anche di capacità di rilevamento, contenimento e risposta. L'azione di sistema deve pertanto 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. La sicurezza è uno di quegli ambiti in cui il grado di strutturazione delle azioni da compiere assume un ruolo determinante, ai fini della loro efficacia.
Strutturare la cybersecurity significa per prima cosa dotare ogni dominio di azione di precisi fondamenti normativi e regolatori, che rappresentano la guida all'interno della quale gli interventi possono o devono essere assunti. Siamo in un caso in cui è necessario prevedere delle norme, che non delineano solo principi e linee programmatiche, ma definiscono vere e proprie strategie, per poi declinarle, attraverso provvedimenti che introducono norme tecniche e tecnologiche, in un'accezione operativa.
Il ruolo degli standard, assieme alle norme di carattere nazionale e comunitario, è pertanto centrale. Sebbene il panorama degli standard di sicurezza sia vastissimo – come del resto sconfinata è la materia – il binomio *norme e standard* permette di raggiungere un quadro organico e ordinato, offrendo punti di riferimento precisi e percorsi di intervento codificati.
Conformità rispetto a standard e norme quindi non significa, per una organizzazione, soltanto tutela rispetto a sanzioni o responsabilità, ma anche capacità di definizione e di pianificazione delle strategie di cybersecurity e delle azioni conseguenti in modo corretto e completo, capacità di monitorare l'adozione delle strategie in ogni fase, misurandone il grado di attuazione e la loro efficacia, nonché capacità di poter dimostrare la maturità delle proprie strategie di fronte a terzi.
Quest'ultimo aspetto si fonda su due pilastri, tra di loro saldamente connessi: la *certificazione* e l'accreditamento. Questo rapporto mira quindi a mostrare quanto *certificazione* e *accreditamento* sviluppino una funzione portante nell'ambito della cybersecurity. Funzione che irrinunciabilmente deve assicurare affidabilità all'intero processo, a tutte le sue componenti, e con essa anche quel necessario grado di standardizzazione, misurabilità, interoperabilità, controllo e leggibilità delle strategie e tattiche adottate.
Il rapporto parte da un'approfondita analisi del panorama normativo e regolatorio nel capitolo 2 che rappresenta la base dell'azione. In questa analisi, riferendosi soprattutto al panorama nazionale e comunitario, viene presentato lo stato dell'arte sulla normativa e sui regolamenti:

l'obiettivo non è solo quello di offrire un quadro di riferimento, ma anche di legare l'azione normativa e regolatoria con gli aspetti e i requisiti di certificazione che essa stessa disciplina. Tra i diversi aspetti trattati, è interessante evidenziare la *Strategia Nazionale di Cybersicurezza* 2022-2026, che ritiene indispensabile il potenziamento del Centro di Valutazione e Certificazione Nazionale (CVCN) dell'Agenzia Nazionale per la Cybersicurezza e dei Centri di Valutazione (CV) del Ministero dell'Interno e del Ministero della Difesa, nonché l'integrazione con una rete di *laboratori di prova accreditati*. Tale potenziamento permetterà di sviluppare capacità nazionali di valutazione delle vulnerabilità di tecnologie a servizio degli asset più critici del Paese. Oltre a definire un quadro giuridico nazionale aggiornato e coerente in materia di cybersecurity, la strategia introduce un insieme di Linee Guida, *schemi di certificazion*e e policy settoriali rivolte ai soggetti pubblici e agli operatori privati.

Il capitolo 3 si concentra sulle nozioni di certificazione e accreditamento attraverso l'analisi delle certificazioni rilevanti nel dominio della cybersecurity e dei relativi processi di accreditamento. L'analisi è condotta a largo spettro e include, tra le altre cose, il dominio della tutela e della protezione dei dati e il dominio delle identità e delle firme elettroniche, nel quadro di riferimento europeo che i due rispettivi regolamenti europei (GDPR ed eIDAS) hanno definito. L'obiettivo non è solo quello di fornire una visione ampia e concreta delle certificazioni rilevanti in ambito di cybersecurity, ma anche quello di far comprendere i benefici derivanti dai processi di certificazione e accreditamento. Inoltre, in questa fase dell'analisi, il rapporto evidenzia il ruolo di ispezione e di vigilanza che il processo di accreditamento attribuisce agli Enti preposti.

I capitoli 4 e 5 si concentrano sugli obiettivi generali del rapporto, vale a dire l'analisi della relazione che esiste tra cybersecurity, certificazione e accreditamento. Tuttavia, l'analisi è fatta da una prospettiva radicalmente nuova, meno disciplinare e più sperimentale. La domanda che gli autori si sono posti nel condurre la ricerca, domanda che trova appunto esplicazione e declinazione nei suddetti capitoli, è stata: dal punto di vista disciplinare non vi è alcun dubbio circa gli effetti benefici della certificazione e dell'accreditamento nell'ambito della cybersecurity, ma è possibile identificare una metodologia, dapprima, e un insieme di indicatori qualitativi e/o quantitativi, successivamente, che possano fornire non solo prova di questo asserto, ma anche un modo per *misurare* il grado di questi benefici?

A tal fine, il rapporto propone e adotta due metodologie. La prima (descritta nel capitolo 4) utilizza il metodo della survey. In questo caso, lo sforzo si è concentrato nella accurata definizione delle domande da sottoporre agli stakeholder selezionati e che meglio potessero offrire un quadro significativo. Gli indicatori ottenuti attraverso questa metodologia sono di natura qualitativa.

La seconda metodologia si è attuata sul campo e si è concretizzata attraverso alcune 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 con la loro postura, in termini di certificazione di cybersecurity (in particolare, secondo la norma tecnica ISO/IEC 27001) e di ulteriori caratteristiche dell'organizzazione. L'analisi, riportata in maniera completamente anonima, ha offerto indicatori di carattere quantitativo che hanno permesso di trarre conclusioni coerenti con le premesse e con l'analisi disciplinare della tematica.

Infine, nel capitolo 6 vengono prospettati gli sviluppi futuri e auspicabili del ruolo dei servizi accreditati per la cybersecurity alla luce delle iniziative nazionali ed europee, quali, ad esempio, il Cybersecurity Act e la Strategia Nazionale di Cybersicurezza, pubblicata dall'Agenzia per la Cybersicurezza Nazionale (ACN). Il contributo di Accredia è già oggi determinante in diversi ambiti legati alla cybersecurity e il supporto alla Pubblica Amministrazione si sostanzia in una stretta collaborazione con ACN.

2. Analisi del panorama normativo/regolatorio

In questo capitolo viene presentato lo stato dell'arte sulla normativa e sui regolamenti rilevanti in materia di cybersecurity attualmente vigenti nel panorama europeo e nazionale, ponendo particolare attenzione agli aspetti e ai requisiti di certificazione che gli stessi disciplinano. Inoltre, vista la mole di prescrizioni che l'attuale normativa richiede ai soggetti economici (pubblici e privati) degli Stati membri, si intende documentare il ruolo che i fornitori di beni, servizi e processi ICT, certificati sotto accreditamento, hanno nell'aiutare le organizzazioni a raggiungere e comprovare la conformità alla normativa vigente finalizzata a ridurre i rischi di incidenti e attacchi informatici. Le certificazioni che avranno un peso maggiore in tale contesto saranno quelle che garantiranno l'implementazione di misure fisiche, tecniche e organizzative conformi agli standard internazionali relativi alla gestione e alla sicurezza delle informazioni. A questo proposito, si intuisce come in futuro aumenterà sempre più la richiesta di aderenza a *schemi di certificazione* con validità nazionale (es. l'attuazione del cloud italiano, con la definizione del modello per la classificazione dei dati e dei servizi della PA e i requisiti per le infrastrutture digitali e per i servizi cloud destinati a trattare dati e servizi strategici, critici e ordinari) e, soprattutto, con validità europea, come la certificazione GDPR (cfr. sezione 2.10) e la EUCS - Certification Scheme per i Cloud Service Provider (cfr. sezione 2.4.2). Molte delle fonti normative qui analizzate appartengono all'attuale architettura nazionale ed europea in tema di organi di certificazione per la cybersecurity, che vede la European Union Agency for Cybersecurity (ENISA), come Ente di riferimento per gli Stati membri dell'UE, e l'Agenzia Nazionale per la Cybersicurezza (ACN), come l'Autorità nazionale di competenza.

La **European Union Agency for Cybersecurity (ENISA)** è un centro di competenze in materia di sicurezza informatica in Europa. Chiamata originariamente *Agenzia europea per la sicurezza delle reti e dell'informazione*, ha assunto il nome attuale il 28 giugno 2019 con il Regolamento UE 2019/881 [2.1][8] (anche conosciuto come EU Cybersecurity Act). Tale Regolamento prevede, tra l'altro, che ENISA assista la Commissione *nelle funzioni di segretariato del gruppo europeo per la certificazione della cybersecurity (ECCG) e provveda alle funzioni di segretariato del gruppo dei portatori di interessi per la certificazione della cybersecurity (SCCG)*.
In breve, l'ENISA 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, e 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 cybersecurity. L'attuale struttura organizzativa di ENISA prevede uno specifico gruppo di lavoro (MCS) per la materia di certificazione e standardizzazione, con particolare riferimento alla cybersecurity (CCS).

[8] *Con [X.X] si indicano i riferimenti bibliografici alla fine del rapporto.*

L'architettura nazionale italiana di cybersecurity è definita nel DL 82/2021 [2.12] convertito con modificazioni dalla Legge 109/2021 [2.14], che istituisce l'Agenzia per la Cybersicurezza Nazionale (ACN) [2.2]. In particolare, il Decreto definisce il Sistema nazionale di sicurezza cibernetica che ha al suo vertice il Presidente del Consiglio dei Ministri al quale è attribuita l'alta direzione e la responsabilità generale delle "politiche di cybersicurezza" e al quale spetta l'adozione della relativa strategia nazionale. Inoltre, allo stesso Presidente, previa deliberazione del Consiglio dei Ministri, spetta la nomina e la revoca del direttore generale e del vicedirettore generale dell'ACN; di tali nomine sono preventivamente informati il Comitato Parlamentare per la Sicurezza della Repubblica (COPASIR) e le competenti Commissioni parlamentari.
Presso la Presidenza del Consiglio dei Ministri è istituito il Comitato Interministeriale per la Cybersicurezza (CIC), organismo con funzioni di consulenza, proposta e vigilanza in materia di politiche di cybersecurity. All'ACN è attribuita, tra l'altro, la funzione di Autorità nazionale di certificazione della cybersicurezza (National Cybersecurity Certification Authority - NCCA), ai sensi dell'art. 58 del Regolamento UE 2019/881 e quindi di tutte le funzioni in materia di certificazione di sicurezza cibernetica, ivi comprese quelle relative al Perimetro di Sicurezza Nazionale Cibernetica (PSNC); tra queste ultime, le funzioni del Centro di Valutazione e Certificazione Nazionale (CVCN), le attività di ispezione e verifica, nonché quelle relative all'accertamento delle violazioni e all'irrogazione delle sanzioni amministrative (attività di vigilanza). Inoltre, ai sensi del Regolamento UE 2019/881, all'ACN sono attribuite le funzioni di accreditamento (art. 60, comma 1) delle strutture specializzate del Ministero della Difesa e del Ministero dell'Interno (i Centri di Valutazione) quali organismi di valutazione della conformità per i sistemi di rispettiva competenza, e di delega (art. 56, comma 6, lettera b) al Ministero della Difesa e al Ministero dell'Interno, attraverso le rispettive strutture accreditate, del rilascio del certificato europeo di sicurezza cibernetica.

Fino alla data di costituzione dell'ACN le funzioni in materia di certificazione di sicurezza cibernetica erano attribuite all'Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione (ISCOM) operante presso il Ministero dello Sviluppo Economico, all'interno del quale era stato istituito l'**Organismo di Certificazione della Sicurezza Informatica (OCSI)** al quale erano attribuite le funzioni di certificazione dal DPCM 30 ottobre 2003 "Schema nazionale per la valutazione e la certificazione della sicurezza nel settore della tecnologia dell'informazione".
Con l'entrata in vigore del DPCM 15 giugno 2022, a partire dal 1° luglio 2022 le funzioni dell'OCSI sono trasferite all'ACN. Pertanto, le richieste di nuove certificazioni di sicurezza secondo lo standard Common Criteria, le richieste di nuovi accertamenti di conformità di dispositivi di firma al Regolamento UE 910/2014 (eIDAS), nonché quelle inerenti all'accreditamento dei **Laboratori per la Valutazione della Sicurezza (LVS)** dovranno essere trasmesse all'ACN che ne curerà la relativa istruttoria e l'emissione dei provvedimenti finali.

2.1 Cybersecurity Act

2.1.1 Regolamento UE 2019/881

Il Regolamento UE 2019/881 [2.1], cosiddetto *Cybersecurity Act* si affianca, ed è in parte complementare, alla prima normativa in materia di sicurezza cibernetica introdotta a livello dell'Unione, ossia la Direttiva NIS. Il Regolamento nasce con un duplice obiettivo: da un lato rafforzare il ruolo di ENISA e, dall'altro, creare un quadro europeo per la certificazione della sicurezza informatica di prodotti ICT e servizi digitali. Il Cybersecurity Act costituisce una parte fondamentale della nuova strategia dell'UE per la sicurezza cibernetica, che mira a rafforzare la resilienza dell'Unione agli attacchi informatici, a creare un mercato unico della sicurezza cibernetica in termini di prodotti, servizi e processi ICT e ad accrescere la fiducia dei consumatori nelle tecnologie digitali.
Come anticipato, un primo punto chiave del Cybersecurity Act riguarda il rafforzamento del ruolo di ENISA. All'Agenzia viene garantito un mandato permanente, permettendo alla stessa di svolgere non solo compiti di consulenza tecnica, ma anche attività di supporto alla gestione operativa degli incidenti informatici da parte degli Stati membri.
Il secondo punto chiave riguarda l'introduzione di un sistema europeo di certificazione della sicurezza informatica dei prodotti e dei servizi digitali, al fine di facilitare lo scambio degli stessi all'interno dell'UE e di accrescere la fiducia dei consumatori nei medesimi. La costituzione di schemi di certificazione specifici per prodotti e sistemi ICT non è una novità. Infatti, numerosi schemi di questo tipo già esistono nella maggior parte degli Stati membri. Ad esempio, in Italia, l'OCSI già certifica la sicurezza informatica di prodotti e sistemi ICT secondo lo schema nazionale per la valutazione e la certificazione della sicurezza nel settore della tecnologia dell'informazione, istituito dal DPCM 30 ottobre 2003 e basato sullo standard internazionale ISO/IEC 15408 [2.13]. Analoghi schemi di certificazione esistono anche in altri Stati membri, come la *Certification de Sécurité de Premier Niveau des Produits des Technologies de l'Information (CSPN)* in Francia, il *Commercial Product Assurance (CPA)* nel Regno Unito e il Baseline Security Product Assessment (BSPA) in Olanda. Tuttavia, molti degli schemi di certificazione nazionale esistenti non vengono riconosciuti al di fuori del Paese che li adotta. Ciò obbliga le organizzazioni a espletare vari processi di certificazione per operare a livello transnazionale.
Il Cybersecurity Act intende ovviare a questi problemi, introducendo 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, ma creando piuttosto un "framework" di base su cui istituire schemi europei per la certificazione. La creazione di questi schemi di certificazione, da predisporsi per specifiche categorie di prodotti e servizi, comporterà che i certificati rilasciati secondo tali schemi saranno validi e riconosciuti in tutti gli Stati membri. Gli schemi europei di certificazione previsti dal Cybersecurity Act saranno predisposti, in prima battuta, dall'ENISA e adottati poi formalmente dalla Commissione europea, mediante atti di esecuzione. Una volta adottato uno schema europeo di certificazione da parte della Commissione, le aziende interessate potranno presentare domanda di certificazione dei propri prodotti o servizi a specifici organismi accreditati, salvo che lo schema di certificazione in questione non consenta alle aziende di procedere a una autovalutazione di conformità (solo per prodotti e servizi a basso rischio). L'utilizzo della certificazione rimarrà però volontario, a meno che la certificazione venga espressamente richiesta per determinate categorie di prodotti o servizi da specifiche norme di settore. Gli schemi europei di certificazione andranno gradualmente a rimpiazzare gli omologhi schemi di certificazione nazionali, che rimarranno validi fino alla loro scadenza naturale.

Lo **European Cybersecurity Certification Group (ECCG)** è il gruppo di lavoro che è stato istituito per aiutare a garantire l'attuazione e l'applicazione del Cybersecurity Act.
In particolare, l'ECCG ha tra i suoi compiti quello di assistere, consigliare e cooperare con l'ENISA in relazione alla preparazione degli schemi di certificazione candidati.
A supporto del lavoro dell'ECCG è stato istituito, sempre da ENISA, lo **Stakeholder Cybersecurity Certification Group (SCCG)**, un gruppo di esperti di certificazione della cybersecurity, che ha il compito di consigliare la Commissione ed ENISA su questioni strategiche riguardanti la certificazione della sicurezza informatica e di assistere la Commissione nella preparazione del programma di lavoro.

L'art. 52 del Regolamento tratta esplicitamente i 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. I requisiti di sicurezza corrispondenti a ogni livello vengono indicati nel sistema europeo di certificazione della cybersecurity pertinente, comprese le corrispondenti funzionalità di sicurezza e il rigore e la specificità corrispondenti alla valutazione a cui deve essere sottoposto il prodotto, servizio o processo ICT. Il certificato o la dichiarazione UE di conformità si riferiscono a specifiche tecniche, norme e procedure ad esso connesse, tra cui i controlli tecnici, il cui obiettivo è ridurre il rischio di incidenti di cybersecurity, o prevenirli.

- Un certificato europeo di cybersecurity o una dichiarazione UE di conformità che si riferisca al livello di affidabilità **"di base"** assicura che i prodotti, i servizi e i processi ICT, per i quali sono rilasciati tali certificati o tali dichiarazioni UE di conformità, rispettino i corrispondenti requisiti di sicurezza (comprese le funzionalità di sicurezza) e siano stati valutati a un livello inteso a *ridurre al minimo i rischi noti di base relativamente a incidenti e attacchi informatici.* Questo è l'unico livello di affidabilità per il quale il sistema europeo di certificazione della cybersecurity può consentire una autovalutazione della conformità sotto la sola responsabilità del fabbricante o del fornitore di prodotti, servizi o processi ICT.

- Un certificato europeo di cybersecurity che fa riferimento a un livello di affidabilità **"sostanziale"** assicura che i prodotti, servizi e processi ICT per i quali è rilasciato tale certificato, rispettino i corrispondenti requisiti di sicurezza, comprese le funzionalità di sicurezza, e siano stati valutati a un livello inteso a *ridurre al minimo i rischi di base noti connessi alla cybersecurity e i rischi di incidenti e di attacchi informatici causati da soggetti dotati di abilità e risorse limitate.* Le attività di valutazione da intraprendere comprendono, almeno, un riesame per dimostrare l'assenza di vulnerabilità pubblicamente note e un test per dimostrare che i prodotti, i servizi o i processi ICT attuino correttamente le necessarie funzionalità di sicurezza; la certificazione di prodotti, servizi e processi ICT per questo livello può essere richiesta solo ad Organismi di certificazione accreditati.

- Un certificato europeo di cybersecurity associato a un livello di affidabilità **"elevato"** assicura che i prodotti, i servizi e i processi ICT per i quali è rilasciato tale certificato rispettino i corrispondenti requisiti di sicurezza, comprese le funzionalità di sicurezza, e siano stati valutati a un livello inteso a *ridurre al minimo il rischio di attacchi informatici avanzati commessi da attori che dispongono di abilità*

e risorse significative. Le attività di valutazione da intraprendere comprendono almeno le seguenti: un riesame per dimostrare l'assenza di vulnerabilità pubblicamente note, un test per dimostrare che i prodotti, i servizi o i processi ICT attuino correttamente le necessarie funzionalità di sicurezza, allo stato tecnologico più avanzato, e una valutazione della loro resistenza agli attacchi commessi da soggetti qualificati mediante test di penetrazione.

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

Per tutti e tre i livelli di affidabilità, qualora le attività di valutazione previste nel Regolamento non siano appropriate, si deve ricorrere ad attività sostitutive di effetto equivalente. Maggiori dettagli in merito al processo adottato da ENISA e dalla Commissione europea per la definizione di uno schema di certificazione europeo si possono trovare sul sito ufficiale del EU Cybersecurity Certification Framework[9].

2.1.2 D.Lgs. 123/2022

Il D.Lgs. 123/2022 adegua l'ordinamento italiano alle disposizioni contenute nel titolo III "Quadro di certificazione della cybersecurity" del Regolamento UE 2019/881. In primo luogo, l'ACN è designata come Autorità nazionale di certificazione della cybersicurezza (art. 4 e art. 7 del DL 52/2021). Con provvedimento del direttore dell'Agenzia, adottato previa consultazione del vicedirettore, saranno definite l'organizzazione e le procedure per lo svolgimento dei compiti a essa assegnati. In particolare, l'ACN svolgerà attività di vigilanza del mercato e rilascio di alcune tipologie di certificati europei di cybersecurity, assicurando che le due funzioni siano svolte da due distinte divisioni. 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'organismo di accreditamento (Accredia) nel monitoraggio e nella vigilanza delle attività degli organismi di valutazione della conformità da essa accreditati. L'Agenzia potrà inoltre avvalersi della collaborazione di altre Autorità di vigilanza del mercato competenti in Italia e negli Stati membri, nonché delle Forze dell'ordine (come previsto, del resto, dall'art. 5 del DL 82/2021). In presenza di una violazione delle disposizioni nazionali e/o comunitarie, l'ACN potrà procedere alla revoca della certificazione e irrogare sanzioni. Nello specifico, l'Agenzia ritirerà direttamente i certificati non conformi con livello di affidabilità elevato, mentre, in caso di certificati non conformi con livelli affidabilità di base o sostanziale in settori chiave (trasporti, energia, banche, finanza, salute, acqua potabile, infrastrutture digitali) chiederà all'organismo emittente di provvedere alla revoca entro cinque giorni e, in caso di inadempienza, procederà motu proprio.

[9] *https://www.enisa.europa.eu/topics/standards/certification*

Per tutti gli altri certificati non conformi, l'Agenzia imporrà all'organismo che ha emesso il certificato di ripetere in tutto o in parte l'attività di valutazione (anche integrando l'attività di valutazione con ulteriori verifiche) al fine di ricondurre il certificato a conformità entro centoventi giorni o di revocarlo. In caso di mancata riconduzione a conformità o mancata revoca del certificato, lo stesso sarà considerato decaduto. Per quanto concerne l'attività di rilascio di certificazioni, occorre operare una distinzione tra i differenti livelli di affidabilità dei certificati richiesti dai sistemi europei: l'ACN è direttamente competente al rilascio di certificazioni con livello di affidabilità elevato e, nello svolgimento di questo compito, si avvale di 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. A tal riguardo, si ricorda che, in base all'art. 7 del DL 82/2021, l'Agenzia ha delegato il Ministero della Difesa e il Ministero dell'Interno al rilascio di certificati europei di cybersecurity, nei rispettivi ambiti di competenza, per il tramite di apposite strutture interne previamente accreditate.

Le certificazioni con livello di affidabilità di base o sostanziale potranno essere rilasciate anche da organismi di valutazione accreditati (da Accredia). In tal caso, l'ACN parteciperà con propri rappresentanti alle deliberazioni sull'accreditamento e l'eventuale revoca o sospensione. Ove un sistema europeo richieda che il rilascio del certificato con livello di affidabilità di base o sostanziale venga effettuato unicamente da parte di organismi di valutazione della conformità pubblici[10], si prevede che gli stessi dovranno essere accreditati (da Accredia), monitorati e designati dall'ACN. I sistemi europei di certificazione possono inoltre prevedere dei requisiti ulteriori o supplementari volti a garantire la competenza tecnica degli organismi di valutazione. In questa fattispecie, l'ACN sarà chiamata ad autorizzare l'attività di tali organismi. Con riferimento ai certificati di livello di affidabilità di base, può essere introdotto (dai sistemi europei) un meccanismo di autovalutazione di conformità da parte dei fornitori e dei fabbricanti di servizi/prodotti ICT, i quali dovranno trasmettere all'ACN tutta la documentazione necessaria per i relativi controlli.

Il D.Lgs. 123/2022, all'art. 8, reca inoltre disposizioni circa l'attività di accreditamento e autorizzazione degli organismi di valutazione della conformità, nonché sull'abilitazione dei laboratori di prova. In particolare, Accredia, nello svolgimento delle funzioni assegnatele dal Regolamento europeo, 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 limitazioni del certificato di accreditamento). L'Agenzia, inoltre, con provvedimento adottato dal direttore generale, sentito il vicedirettore generale, costituirà, 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. All'art. 9, il Decreto disciplina l'attività di ricerca/formazione. Al tal riguardo, si prevede che l'ACN potrà realizzare progetti di ricerca/formativi, ivi inclusi quelli per lo sviluppo di software, avvalendosi della collaborazione di Università, centri di ricerca o laboratori specializzati nel campo della valutazione della sicurezza informatica. Per finanziare tali progetti potranno essere

---

[10] *Ai sensi dell'art. 56, paragrafo 5, del Regolamento UE 2019/881, in casi debitamente giustificati un sistema europeo di certificazione della cybersecurity può prevedere che i certificati europei di cybersecurity derivanti da tale sistema possano essere rilasciati unicamente da un Ente pubblico.*

utilizzati i proventi derivanti dalle sanzioni. A tal proposito, il Decreto dettaglia tutte le fattispecie per le quali sarà attivato il meccanismo sanzionatorio (art. 10). L'art. 9 dispone 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 l'ECCG di ogni intenzione di elaborare nuovi sistemi nazionali di certificazione della cybersecurity. La relazione tra l'ACN e l'ECCG sarà in ogni caso costante, in quanto l'Agenzia parteciperà alle attività internazionali del gruppo europeo (art. 4). Oltre all'attività di ricerca, l'ACN gestirà gli eventuali reclami relativi al rilascio di certificati da parte dell'OCSI o all'autorizzazione di organismi (ove prevista). Le persone fisiche e giuridiche hanno in ogni caso diritto a presentare ricorso all'emittente del certificato e, se del caso, anche all'Autorità giudiziaria.
È inoltre stabilito che le attività di vigilanza, di certificazione, di autorizzazione, di abilitazione saranno sottoposte a tariffa, da calcolarsi sulla base dei costi effettivi dei servizi resi. I relativi proventi saranno versati ad apposito capitolo dell'entrata del bilancio dello Stato per essere successivamente riassegnati, con Decreto del Ministro dell'Economia e delle Finanze, sul pertinente capitolo dello stato di previsione della spesa del Ministero stesso, per incrementare la dotazione degli appositi capitoli dell'Agenzia.
Si evidenzia infine come, ove nuovi sistemi europei di certificazione non siano autonomamente applicabili nel quadro di certificazione nazionale vigente, l'ACN dovrà dare piena attuazione alle norme comunitarie, modificando e integrando il provvedimento del direttore generale contenente le procedure per lo svolgimento dei compiti dell'Agenzia.

2.2 Direttive per Infrastrutture Critiche - NIS e NIS2

2.2.1 Direttiva EU 2016/1148 (NIS)

La Direttiva sulla sicurezza delle reti e delle informazioni (Direttiva EU 2016/1148 [2.3]) nota come *NIS (Network and Information Security*) è stata emanata dalla Commissione europea come parte della strategia di cybersecurity dell'Unione. La Direttiva NIS 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, imponendo agli Stati membri una serie di obblighi, tradotti in misure di sicurezza, per conseguire un livello comune elevato di sicurezza della rete e dei sistemi informativi nella UE. A tal fine:

1. fa obbligo a tutti gli Stati membri di adottare una strategia nazionale in materia di sicurezza della rete e dei sistemi informativi;
2. istituisce un gruppo di cooperazione (NIS Cooperation Group) al fine di sostenere e agevolare la cooperazione strategica e lo scambio di informazioni tra Stati membri e di sviluppare la fiducia tra di essi;
3. crea una rete di gruppi di intervento per la sicurezza informatica in caso di incidente ("rete degli CSIRT") per contribuire allo sviluppo della fiducia tra Stati membri e promuovere una cooperazione operativa rapida ed efficace;
4. stabilisce obblighi di sicurezza e di notifica per gli operatori di servizi essenziali e per i fornitori di servizi digitali;

5. fa obbligo agli Stati membri di designare Autorità nazionali competenti, punti di contatto unici e CSIRT con compiti connessi alla sicurezza della rete e dei sistemi informativi.

Si compone principalmente di tre parti:

1. **Capacità nazionali**: gli Stati membri dell'UE devono avere determinate capacità nazionali di cybersecurity, come un Computer Security Incident Response Team (CSIRT) nazionale, attività di esercitazione cibernetiche, ecc.
2. **Collaborazione transfrontaliera**: collaborazione transfrontaliera tra i Paesi dell'UE, ad esempio attraverso la rete operativa CSIRT dell'UE, il gruppo di cooperazione strategica NIS, etc.
3. **Supervisione nazionale dei settori critici**: gli stati membri dell'UE devono supervisionare la cybersecurity degli operatori critici del mercato nel loro Paese. La supervisione deve avvenire *ex-ante* nei settori critici (energia, trasporti, acqua, salute, infrastrutture digitali e settore finanziario) ed *ex-post* per i fornitori di servizi digitali critici (mercati online, cloud e motori di ricerca online).

Essendo una Direttiva, offre ai Paesi dell'UE un certo livello di flessibilità per tenere conto delle circostanze nazionali, ad esempio, per riutilizzare le strutture organizzative esistenti o per allinearsi alla legislazione nazionale esistente. Adottata a partire dal 2016, è stata recepita da parte degli Stati membri dell'UE il 9 maggio 2018: in Italia è stata recepita con il D.Lgs. 65/2018 [2.5].

2.2.2 Proposta della Direttiva EU NIS2

La proposta della Direttiva EU NIS2 [2.4] 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'UE nel suo complesso, nel campo della cybersecurity 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. La NIS2 si basa e abroga la Direttiva EU 2016/1148 (NIS) e prevede misure giuridiche volte a incrementare il livello complessivo di cybersecurity nell'Unione. In particolare, la NIS2 cerca di migliorare la vecchia NIS partendo dalle esperienze positive e negative di quest'ultima, modernizzando il quadro giuridico esistente, tenendo conto della crescente digitalizzazione del mercato interno avvenuta negli ultimi anni e del panorama in rapida evoluzione delle minacce cyber, che vede gli attacchi informatici in continuo aumento, molti dei quali, sempre più sofisticati e per lo più provenienti da un'ampia gamma di fonti interne ed esterne all'UE.

2.3 Direttive per specifici domini

2.3.1 Regolamento UE 910/2014 (eIDAS)

Il Regolamento UE 910/2014 noto come eIDAS *(electronic IDentification Authentication and Signature)* [2.25] ha l'obiettivo di creare il substrato di regole cogenti, valide in tutta l'Unione europea, in merito all'identificazione elettronica delle persone fisiche e giuridiche, nonché

all'erogazione sicura di servizi fiduciari, quali la firma o il sigillo elettronico di documenti, la marcatura temporale (che consente di stabilire in modo univoco il momento nel quale un documento è stato prodotto), la conservazione di firme e sigilli, nonché altri servizi come quelli di validazione delle firme e sigilli e la cosiddetta "Posta Elettronica Certificata Europea", altresì nota come *Registered Electronic Mail* (REM), e i servizi relativi ai certificati di autenticazione dei siti web. Il Regolamento fornisce un elevato livello di garanzia a supporto della fiducia che i cittadini, le imprese e le Pubbliche Amministrazioni attribuiscono alle transazioni elettroniche, ponendo al centro la sicurezza ICT. Per offrire adeguata garanzia, i fornitori dei servizi fiduciari (*Trust Service Providers*) vengono "qualificati" dalle Autorità nazionali e rispondono, entro limiti contrattualmente definiti, per i possibili danni provocati a persone fisiche o giuridiche a causa del mancato rispetto degli obblighi previsti dal Regolamento stesso. Il percorso di qualifica, che permette di inserire i Trust Service Providers in liste di soggetti notificati a livello UE, prevede una fase istruttoria, che si avvale dell'operato di organismi di certificazione appositamente accreditati. Il Regolamento eIDAS sostituisce e integra la precedente Direttiva 1999/93/EC, che riguardava alcuni dei servizi fiduciari, oggi ampliati e prossimi a ulteriori integrazioni con la revisione del Regolamento. Il Regolamento fissa le condizioni per il riconoscimento reciproco tra gli Stati membri dei sistemi di identificazione elettronica – come il Sistema Pubblico di identità Digitale italiano (SPID) – sviluppati sulla base di requisiti specifici, previa notifica fatta dall'Autorità di Sorveglianza di un Paese membro a tutti gli altri Stati. In Italia, tale Autorità è rappresentata dall'Agenzia per l'Italia Digitale (AgID). Per meglio comprendere la portata degli effetti del Regolamento eIDAS occorre sottolineare come, a oggi, il servizio SPID italiano sia riconosciuto e funzionante praticamente in tutta l'Unione Europea. Questo avviene tramite il "nodo di interoperabilità eIDAS" creato dallo Stato italiano, così come simili infrastrutture sono state realizzate (o sono in via di completamento) negli altri Stati membri dell'Unione. L'interconnessione avviene sulla base dei requisiti del programma *Connecting Europe Facility* (CEF) recepiti e applicati dall'AgID, con il supporto di alcuni partner tecnologici. L'identificazione sicura del cittadino è garantita da SPID o dall'uso della Carta d'Identità Elettronica (CIE). Le Amministrazioni nazionali hanno iniziato a consentire l'accesso del cittadino, tramite SPID e CIE, a molteplici servizi, che andranno a estendersi sempre di più. Questo applicazione può essere adottata anche da operatori privati, che possono così usufruire dell'identificazione sicura dei propri utenti. Il nodo di interoperabilità eIDAS è una struttura server, che permette la connessione reciproca degli utenti eIDAS nei Paesi dell'Unione europea. Il nodo garantisce la gestione sicura delle identità scambiate o utilizzate sulle reti telematiche a livello UE, previo l'utilizzo di browser che imbarchino certificati di sicurezza validi – anch'essi realizzati secondo le regole eIDAS condivise con il consorzio volontario degli operatori di crittografia web (*CA Browser Forum*) – e garantisce il valore legale delle comunicazioni e degli atti, identificando gli utenti e le controparti.

2.3.2 Schema di certificazione europea dei servizi cloud (EUCS)

Nel contesto della definizione degli *schemi di certificazione europei sulla cybersecurity*, ENISA ha elaborato la versione draft dello schema di certificazione dei servizi cloud dell'Unione europea ***European Union Cybersecurity Certification Scheme on Cloud Services*** **(EUCS)** la cui revisione esterna si è conclusa il 7 febbraio 2021. Lo schema ha l'obiettivo di armonizzare la sicurezza dei servizi cloud con i regolamenti dell'UE, gli standard internazionali e le migliori pratiche del settore, così come con le certificazioni già esistenti negli Stati membri.

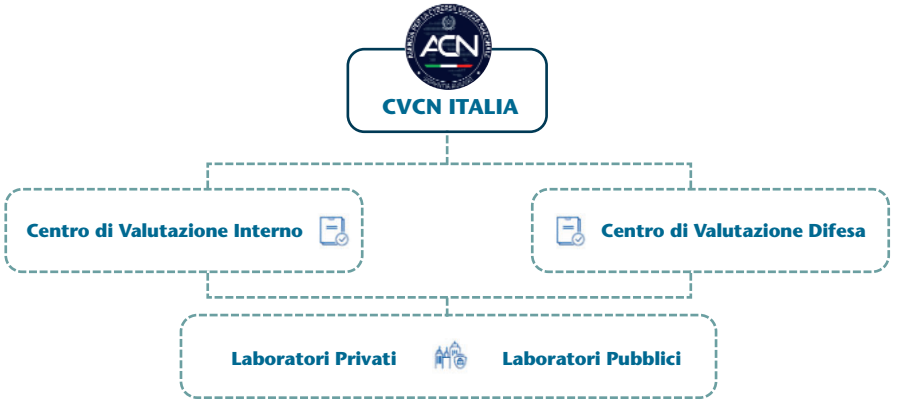
2.4 Strategia Nazionale di Cybersicurezza 2022-2026

Il 18 maggio 2022, con approvazione del Comitato Interministeriale per la Cybersecurity, l'ACN ha emanato la *Strategia Nazionale di Cybersicurezza 2022-2026* volta a pianificare, coordinare e attuare misure tese a rendere il Paese più sicuro e resiliente agli attacchi cyber. La Strategia individua tre obiettivi fondamentali da perseguire, ossia *protezione, risposta e sviluppo* con la definizione di un insieme di 82 misure, contenute nell'annesso *Piano di implementazione*, intese ad assicurare la concreta attuazione della Strategia. L'obiettivo 1 della Strategia (*protezione degli asset strategici nazionali*) pone particolare attenzione allo *sviluppo di strategie e iniziative per la verifica e valutazione della sicurezza delle infrastrutture ICT*, ivi inclusi gli aspetti di approvvigionamento e *supply chain* a impatto nazionale; sviluppo che viene considerato un elemento cardine per poter assicurare un livello di protezione efficace e duraturo. Infatti, la Strategia ritiene 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) dei Ministeri dell'Interno e della Difesa, nonché l'integrazione con una rete di laboratori di prova accreditati, in quanto tale potenziamento permetterà di sviluppare capacità nazionali di valutazione delle vulnerabilità di tecnologie a servizio degli asset più critici del Paese. La Strategia rafforza la necessità di definire un quadro giuridico nazionale aggiornato e coerente in materia di cybersecurity che tenga conto degli orientamenti e degli sviluppi in ambito europeo e internazionale. Tale quadro, però, non deve ricomprendere solamente il livello normativo, ma anche un insieme di Linee Guida, *schemi di certificazione* e policy settoriali rivolte ai soggetti pubblici e agli operatori privati. In tale contesto, assumono rilevanza primaria, tra l'altro:

- *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.

Figura 2.1 - Schema architetturale dei centri di valutazione e certificazione per il contesto italiano



In merito alle misure contenute nel Piano di implementazione della Strategia, specifiche per il tema di certificazione, vanno evidenziate:

- **Misura #1** prevede di *"Rafforzare il sistema di scrutinio tecnologico nazionale a supporto della sicurezza della supply chain e l'adozione di schemi di certificazione europea di cybersecurity, anche mediante l'accreditamento di laboratori di valutazione pubblico/privati"*.

- **Misura #2** propone di *"Sviluppare le capacità dei Centri di Valutazione del Ministero dell'Interno e del Ministero della Difesa accreditati dall'ACN, quali organismi di valutazione della conformità, per i sistemi di rispettiva competenza*".

- **Misura #5** intesa a *"Supportare lo sviluppo, valutandone l'adeguatezza in termini di sicurezza nazionale, degli schemi di certificazione in materia di cybersecurity e, in collaborazione con il settore privato, promuoverne l'adozione e l'utilizzo da parte dei fornitori di servizi e delle imprese italiane, favorendo lo sviluppo del tessuto imprenditoriale nazionale specializzato al fine di conseguire un vantaggio competitivo sul mercato"*.

- **Misura #61** mira a *"Sviluppare 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 mantiene una lista dei percorsi di formazione, approvati dalla stessa Agenzia, al termine dei quali il discente consegue, oltre al titolo di studio/professionale, la relativa certificazione"*.

2.5 Perimetro di Sicurezza Nazionale Cibernetica

La normativa nazionale 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. L'obiettivo, tra l'altro, è definire un'architettura organizzativa e operativa e un piano strategico della sicurezza cibernetica nazionale, al fine di assicurare *"un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori nazionali, pubblici e privati, da cui dipende l'esercizio di una funzione essenziale dello Stato, ovvero la prestazione di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato e dal cui malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale"*.
La normativa sul PSNC è stata sottoposta a recente aggiornamento mediante DL 82/2021 [2.12] convertito con modificazioni nella Legge 109/2021 [2.14], in cui si individua l'ACN come l'Ente di riferimento in materia di sicurezza nazionale cibernetica.

2.5.1 D.Lgs. 65/2018

Il D.Lgs. 65/2018 attua la Direttiva NIS [2.5] nel contesto italiano, stabilendo le Autorità competenti NIS per i settori e sottosettori di cui all'allegato II e per i servizi di cui all'allegato III del NIS, ossia:

a) il Ministero dello Sviluppo Economico per il settore energia, sottosettori energia elettrica, gas e petrolio e per il settore infrastrutture digitali, sottosettori IXP, DNS, TLD, nonché per i servizi digitali;
b) il Ministero delle Infrastrutture e dei Trasporti per il settore trasporti, sottosettori aereo, ferroviario, per vie d'acqua e su strada;
c) il Ministero dell'Economia e delle Finanze per il settore bancario e per il settore infrastrutture dei mercati finanziari, in collaborazione con le Autorità di vigilanza di settore, Banca d'Italia e Consob, secondo modalità di collaborazione e di scambio di informazioni stabilite con decreto del Ministro dell'Economia e delle Finanze;
d) il Ministero della Salute per l'attività di assistenza sanitaria, come definita dall'art. 3, comma 1, lettera a), del D.Lgs. 38/2014, prestata dagli operatori dipendenti o incaricati dal medesimo Ministero o convenzionati con lo stesso e le Regioni e le Province autonome di Trento e di Bolzano, direttamente o per il tramite delle Autorità sanitarie territorialmente competenti, per le attività di assistenza sanitaria prestata dagli operatori autorizzati e accreditati delle Regioni o dalle Province autonome negli ambiti territoriali di rispettiva competenza;
e) il Ministero dell'Ambiente e della Tutela del Territorio e del Mare e le Regioni e le Province autonome di Trento e di Bolzano, direttamente o per il tramite delle Autorità territorialmente competenti, in merito al settore fornitura e distribuzione di acqua potabile.

Le Autorità competenti NIS hanno l'obbligo di individuare, per ciascun settore e sottosettore di propria competenza, gli *Operatori di Servizi Essenziali* (OSE) con una sede nel territorio nazionale. I criteri per l'identificazione degli operatori di servizi essenziali sono:

a) un soggetto fornisce un servizio che è essenziale per il mantenimento di attività sociali e/o economiche fondamentali;
b) la fornitura di tale servizio dipende dalla rete e dai sistemi informativi;
c) un incidente avrebbe effetti negativi rilevanti sulla fornitura di tale servizio.

L'ACN è designata quale punto di contatto unico in materia di sicurezza delle reti e dei sistemi informativi, secondo quanto stabilito dal DL 82/2021 convertito dalla Legge 109/2021. Come punto di contatto unico, svolge una funzione di collegamento per garantire la cooperazione transfrontaliera delle Autorità competenti NIS con le Autorità competenti degli altri Stati membri, nonché con il gruppo di cooperazione di cui all'art. 10 (rappresentanti degli Stati membri, della Commissione europea e dell'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione) e la rete di CSIRT di cui all'art. 11 (composta da rappresentanti dei CSIRT degli Stati membri e del CERT-UE). Il Decreto, inoltre, istituisce, presso la Presidenza del Consiglio dei Ministri, il CSIRT italiano, che svolge i compiti e le funzioni del Computer Emergency Response Team (CERT) nazionale, di cui all'art. 16-bis del D.Lgs. 259/2003, e del CERT-PA, già operante presso l'AgID ai sensi dell'art. 51 del D.Lgs. 82/2005. Il CSIRT italiano è stato trasferito con la Legge 109/2021 presso l'ACN, assumendo la denominazione di **CSIRT Italia**.

Sempre attraverso il Decreto, viene istituito, presso il Ministero dello Sviluppo Economico, un elenco nazionale degli operatori di servizi essenziali. Tale elenco viene aggiornato almeno ogni due anni; l'aggiornamento spetta alle Autorità competenti NIS e deve essere comunicato al Ministero dello Sviluppo Economico.
Gli operatori di servizi essenziali e i fornitori di servizi digitali sono tenuti a inviare le notifiche relative a incidenti di propria competenza al CSIRT Italia, che, a sua volta, informa le Autorità competenti NIS e il punto di contatto unico (ACN) in merito alle notifiche di incidenti trasmesse. Le notifiche includono le informazioni che consentono al CSIRT Italia di determinare un eventuale impatto transfrontaliero dell'incidente e, nel caso, di informare gli eventuali altri Stati membri interessati. Le Autorità competenti NIS possono predisporre Linee Guida per la notifica degli incidenti.

2.5.2 DL 105/2019 coordinato con Legge 133/2019

Il DL 105/2019 [2.6], convertito, con modificazioni, dalla Legge 133/2019 [2.7], prevede "Disposizioni urgenti in materia di Perimetro di Sicurezza Nazionale Cibernetica (PSNC) e di disciplina dei poteri speciali nei settori di rilevanza strategica". La norma ha lo scopo di contribuire alla sicurezza nazionale proteggendo reti, sistemi informativi, servizi informatici di amministrazioni pubbliche, Enti e operatori pubblici e privati aventi una sede nel territorio nazionale da cui dipendono *funzioni essenziali* per lo Stato o *servizi essenziali* per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato (art. 1). Il Decreto rimanda a due successivi decreti attuativi (art. 1 comma 2 e comma 3): il DPCM 131/2020 (DPCM I) e il DPCM 81/2021 (DPCM II).

In sintesi, il DL 105/2019 prevede che:

a) siano individuati le Amministrazioni Pubbliche, gli Enti e gli operatori pubblici e privati aventi una sede nel territorio nazionale, rientranti nel PSNC (già DPCM II);
b) siano definiti, sulla base di un'analisi del rischio e di un criterio di gradualità che tenga conto delle specificità dei diversi settori di attività, i criteri con i quali i soggetti del PSNC predispongono e aggiornano, con cadenza almeno annuale, un elenco delle reti, dei sistemi informativi e dei servizi informatici, di rispettiva pertinenza, comprensivo della relativa architettura e componentistica. Tali soggetti del perimetro sono tenuti al rispetto di particolari misure e obblighi in materia di sicurezza cibernetica (già DPCM II);
c) siano definite le procedure secondo cui i soggetti del PSNC notificano gli incidenti aventi impatto su reti, sistemi informativi e servizi informatici, al Gruppo di intervento per la sicurezza informatica in caso di incidente di CSIRT Italia;
d) siano stabilite misure volte a garantire elevati livelli di sicurezza delle reti, dei sistemi informativi e dei servizi informatici a supporto delle funzioni e dei servizi essenziali;
e) siano disciplinate le procedure, le modalità e i termini con cui i soggetti rientranti nel PSNC – ovvero le centrali di committenza alle quali essi fanno ricorso ai sensi dell'art. 1, comma 512, della Legge 208/2015, che intendano procedere all'affidamento di forniture di beni, sistemi e servizi ICT destinati a essere impiegati sulle reti, sui sistemi informativi e per l'espletamento dei servizi informatici a supporto delle funzioni e dei servizi essenziali e appartenenti a categorie individuate con decreto del Presidente del Consiglio dei Ministri – ne danno comunicazione al Centro di Valutazione e Certificazione Nazionale (CVCN), istituito presso l'ACN.

In relazione alla specificità delle forniture di beni, sistemi e servizi ICT da impiegare su reti, sistemi informativi e servizi informatici del Ministero dell'Interno e del Ministero della Difesa, i predetti Ministeri, in coerenza con quanto previsto dal Decreto, possono procedere, con le medesime modalità e i medesimi termini precedentemente descritti, attraverso la comunicazione ai propri Centri di Valutazione accreditati per le attività di valutazione, che impiegano le metodologie di verifica e di test definite dal CVCN. Per tali casi, i Centri di Valutazione accreditati informano il CVCN.

2.5.3 DPCM 131/2020 (DPCM I)

Il DPCM 131/2020 (DPCM I) [2.8] definisce le modalità e i criteri procedurali di individuazione dei soggetti pubblici e privati inclusi nel PSNC, nonché i criteri con i quali i soggetti inclusi nel perimetro predispongono e aggiornano un elenco delle reti, dei sistemi informativi e dei servizi informatici di rispettiva pertinenza. Secondo il provvedimento, un soggetto esercita una funzione essenziale dello Stato *"laddove l'ordinamento gli attribuisca compiti rivolti ad assicurare la continuità dell'azione di Governo e degli Organi costituzionali, la sicurezza interna ed esterna e la difesa dello Stato, le relazioni internazionali, la sicurezza e l'ordine pubblico, l'amministrazione della giustizia, la funzionalità dei sistemi economico e finanziario e dei trasporti"*. Un soggetto, pubblico o privato, presta un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato, laddove ponga in essere *"attività strumentali all'esercizio di funzioni essenziali dello Stato; attività necessarie per l'esercizio e il godimento dei diritti fondamentali; attività necessarie per la continuità degli approvvigionamenti e l'efficienza delle infrastrutture e della logistica; attività di ricerca e attività relative alle realtà produttive nel campo dell'alta tecnologia e in ogni altro settore, ove presentino rilievo economico e sociale, anche ai fini della garanzia dell'autonomia strategica nazionale, della competitività e dello sviluppo del sistema economico nazionale*".
In prima istanza, i soggetti inclusi nel PSNC sono quelli operanti nel settore governativo, nell'ambito delle attività dell'Amministrazione dello Stato e delle attività delle Amministrazioni appartenenti al Comitato Interministeriale per la Sicurezza della Repubblica (CISR), nonché gli ulteriori soggetti, pubblici o privati, operanti nei seguenti settori di attività, ove non ricompresi in quello governativo (comunque in riferimento ad amministrazioni centrali):

- interno, con competenza del Ministero dell'Interno;
- difesa, con competenza del Ministero della Difesa;
- spazio e aerospazio, con competenza della Presidenza del Consiglio dei Ministri;
- energia e telecomunicazioni, con competenza del Ministero dello Sviluppo Economico;
- economia e finanza, con competenza il Ministero dell'Economia e delle Finanze;
- trasporti, con competenza del Ministero delle Infrastrutture e dei Trasporti;
- servizi digitali, con competenza del Ministero dello Sviluppo Economico, in raccordo con la struttura della Presidenza del Consiglio dei Ministri competente per l'innovazione tecnologica e la digitalizzazione;

- tecnologie critiche, con competenza della struttura della Presidenza del Consiglio dei Ministri competente per l'innovazione tecnologica e la digitalizzazione, in raccordo con il Ministero dello Sviluppo Economico e con il Ministero dell'Università e della Ricerca;

- enti previdenziali/lavoro, con competenza del Ministero del Lavoro e delle Politiche Sociali.

Le Amministrazioni sopra individuate, in relazione ai settori di attività di competenza:

a) identificano le funzioni essenziali e i servizi essenziali di diretta pertinenza, ovvero esercitati o prestati da soggetti vigilati o da operatori anche privati, che dipendono da reti, sistemi informativi o servizi informatici, la cui interruzione o compromissione possa arrecare un pregiudizio per la sicurezza nazionale;
b) valutano a tali fini:
   1. gli effetti di una interruzione della funzione essenziale o del servizio essenziale, rispetto all'estensione territoriale della funzione o del servizio, al numero e alla tipologia di utenti potenzialmente interessati, ai livelli di servizio garantiti, ove previsti, alle possibili ricadute economiche, ove applicabili, e ogni altro elemento rilevante;
   2. gli effetti della compromissione dello svolgimento della funzione essenziale o del servizio essenziale rispetto alle conseguenze della perdita di disponibilità, integrità o riservatezza dei dati e delle informazioni trattati per il loro svolgimento, avuto riguardo della tipologia e della quantità degli stessi, alla loro sensibilità ed allo scopo cui sono destinati;
   3. la possibile mitigazione, rispetto all'interruzione o alla compromissione dello svolgimento della funzione essenziale o del servizio essenziale, in relazione al tempo necessario per ripristinarne lo svolgimento in condizioni di sicurezza e alla possibilità che lo svolgimento della funzione essenziale o del servizio essenziale possano o meno essere assicurati, anche temporaneamente, con modalità prive di supporto informatizzato ovvero anche parzialmente da altri soggetti;
c) individuano le funzioni essenziali e i servizi essenziali per i quali in caso di interruzione o compromissione, il pregiudizio per la sicurezza nazionale è ritenuto massimo e le possibilità di mitigazione minime, e li graduano in una scala crescente;
d) individuano i soggetti che svolgono le funzioni essenziali o i servizi essenziali di cui alla lettera c). In fase di prima applicazione sono individuati i soggetti titolari delle funzioni essenziali o dei servizi essenziali che in caso di un'interruzione delle attività comporterebbero il mancato svolgimento della funzione o del servizio.

Le Amministrazioni competenti per la cybersecurity, in relazione ai settori di attività di competenza, predispongono, per la sottoposizione al CISR, una lista di soggetti e la trasmettono al CISR tecnico. A supporto del CISR tecnico è istituito il "Tavolo interministeriale" per l'attuazione del PSNC.

2.5.4 DPCM 81/2021 (DPCM II)

Il DPCM 81/2021 (DPCM II) [2.9] specifica le modalità e il contenuto delle comunicazioni degli incidenti, da parte dei soggetti appartenenti al PSNC ed elenca 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 da esso inseriti in appositi elenchi.

Il DPCM II, agli artt. 2, 3, 4, propone una classificazione degli incidenti cyber accompagnata dalla modalità di comunicazione degli stessi ai soggetti preposti. In particolare, gli incidenti cyber vengono suddivisi in:

- "meno gravi" (tabella 1 , allegato A) per cui va data comunicazione a CSIRT Italia, entro il termine delle 6 ore dal momento in cui il soggetto incluso nel perimetro è venuto a conoscenza, mediante canale ufficiale;

- "più gravi" (tabella 2, allegato A) per cui va data comunicazione a CSIRT Italia, entro il termine di 1 ora dal momento in cui il soggetto incluso nel perimetro è venuto a conoscenza, mediante canale ufficiale.

Qualora il soggetto incluso nel perimetro venga a conoscenza di nuovi elementi significativi, integra tempestivamente la notifica, salvo che l'Autorità giudiziaria procedente abbia previamente comunicato la sussistenza di specifiche esigenze di segretezza investigativa. Analogamente, salvo che l'Autorità giudiziaria procedente abbia previamente comunicato la sussistenza di specifiche esigenze di segretezza investigativa su richiesta di CSIRT Italia, il soggetto incluso nel perimetro che ha provveduto ad effettuare una notifica procede, tramite gli opportuni canali di comunicazione ed entro 6 ore dalla richiesta, a effettuare un aggiornamento della notifica. Una volta definiti e avviati i piani di attuazione delle attività per il ripristino dei beni ICT impattati dall'incidente oggetto di notifica, il soggetto incluso nel perimetro che ha provveduto a effettuare una notifica, tramite gli opportuni canali di comunicazione, ne dà tempestiva comunicazione al CSIRT Italia e trasmette una relazione tecnica, entro 30 giorni dalla richiesta del CSIRT Italia. La relazione illustra gli elementi significativi dell'incidente, tra cui le conseguenze dell'impatto sui beni ICT derivanti dall'incidente e le azioni intraprese per porvi rimedio, salvo che, anche in questo caso, l'Autorità giudiziaria procedente abbia previamente comunicato la sussistenza di specifiche esigenze di segretezza investigativa.
I soggetti inclusi nel perimetro adottano, per ciascun bene ICT di rispettiva pertinenza, le misure di sicurezza di cui all'allegato B del DPCM e ne comunicano l'avvenuta adozione e le relative modalità, mediante la piattaforma digitale costituita presso il DIS (ora ACN), nei seguenti termini:

a) per le misure di sicurezza appartenenti alla categoria A di cui all'appendice 2 dell'allegato B, entro 6 mesi dalla data di trasmissione degli elenchi dei beni ICT a supporto dello svolgimento delle funzioni o dei servizi essenziali del soggetto incluso nel perimetro, ovvero, qualora la trasmissione avvenga in una data antecedente a quella di entrata in vigore del presente Regolamento, entro 6 mesi da quest'ultima data. Nell'ipotesi in cui le abbiano già adottate, comunicano altresì le modalità di adozione delle misure di sicurezza di cui alla categoria B dell'appendice 2 dell'allegato B;
b) per quelle appartenenti alla categoria B di cui all'appendice 2 dell'allegato B, entro 30 mesi dalla data di trasmissione degli elenchi dei beni ICT a supporto dello svolgimento delle funzioni o dei servizi essenziali del soggetto incluso nel perimetro, ovvero, qualora la trasmissione avvenga in una data antecedente a quella di entrata in vigore del presente regolamento, entro trenta mesi da quest'ultima data.

Qualora un soggetto incluso nel perimetro proceda all'aggiornamento dell'elenco dei beni ICT a supporto dello svolgimento delle funzioni o dei servizi essenziali, valuta contestualmente se sia necessario procedere all'adeguamento delle misure di sicurezza adottate.

Nel caso in cui sia necessario procedere all'adeguamento, vi provvede e ne comunica le relative modalità nei seguenti termini:

a) per le misure di sicurezza di cui alla categoria A dell'appendice 2 dell'allegato B, entro 6 mesi all'aggiornamento dell'elenco dei beni ICT;
b) per le misure di sicurezza di cui alla categoria B dell'appendice 2 dell'allegato B, entro 24 mesi all'aggiornamento dell'elenco dei beni ICT.

Il Decreto disciplina anche le modalità di notifica volontarie, per gli incidenti non riepilogati nelle tabelle del decreto.

2.5.5 DPR 54/2021

Il DPR 54/2021 [2.10] affronta le procedure e i termini per le valutazioni da parte del CVCN e dei CV (Centri di Valutazione) relativi alla materia, rispettivamente del Ministero della Difesa e del Ministero dell'Interno su prodotti in acquisizione da parte dei soggetti inclusi nel PSNC (i CV non vanno confusi con i *Ce.Va. Centri di Valutazione per le certificazioni di sicurezza cibernetica di prodotto* in ambito Common Criteria per i prodotti che operano su dati classificati)
Il Decreto definisce un'articolata procedura di valutazione, ispezione e definizione dei criteri tecnici per l'individuazione delle categorie dei beni e servizi ICT che determinano i rapporti tra i soggetti individuati nel perimetro di sicurezza e le Autorità competenti, con particolare riguardo alle acquisizioni di oggetti di fornitura di beni, sistemi e servizi ICT destinati a essere impiegati sui beni ICT di cui all'elenco dell'art. 7 del DPCM 131/2020 (DPCM I). In particolare, l'art. 3 afferma che i soggetti inclusi nel Perimetro, prima dell'avvio delle procedure di affidamento o prima della conclusione dei contratti relativi alla fornitura di beni, sistemi e di servizi ICT anche nel caso in cui tali procedure siano espletate attraverso le centrali di committenza, ne danno comunicazione al CVCN o ai CV. Di fatto, con il DPR, si rendono operativi il CVCN e i CV, deputati ai procedimenti di verifica e valutazione dei beni, sistemi e servizi ICT utilizzati dalle organizzazioni rientranti nel PSNC.
Nello specifico, il provvedimento è finalizzato all'attuazione dei tre "compiti normativi" previsti dall'art. 1, comma 6 del DL 105/2019 e in particolare:

- definire le procedure, le modalità e i termini a cui i soggetti pubblici e privati inclusi nel perimetro di sicurezza nazionale cibernetica devono attenersi, qualora intendano procedere all'affidamento di forniture di beni, di sistemi e di servizi ICT destinati a essere impiegati sulle reti, sui sistemi informativi e per l'espletamento dei servizi informatici, appartenenti a categorie individuate nel DPCM del 15 giugno 2021 (DPCM III);

- stabilire le procedure, le modalità e i termini con cui i fornitori dei suddetti beni, sistemi e servizi destinati alle reti, ai sistemi e ai servizi rilevanti assicurano la propria collaborazione al CVCN e ai CV (sia del Ministero dell'Interno, sia del Ministero della Difesa) per l'effettuazione dei test richiesti da questi ultimi;

- definire le procedure, le modalità e i termini con i quali il Ministero dello Sviluppo Economico (MISE) e la Presidenza del Consiglio dei Ministri svolgono le attività di ispezione e verifica (funzioni ora attribuite all'ACN).

Il provvedimento prevede che l'esito delle attività di verifica venga comunicato dal CVCN e dai CV ai soggetti verificati, con le eventuali condizioni da inserire nel bando o nel contratto di fornitura del bene o servizio da acquisire.
Il DPR descrive in maniera dettagliata l'intera procedura di valutazione del CVCN e dei CV e in particolare: l'art. 3 descrive la procedura di comunicazione di affidamento da parte del soggetto del perimetro; l'art. 4 dettaglia il procedimento di verifica e valutazione da parte dei centri; l'art. 5 individua le verifiche preliminari eseguite dai centri insieme all'individuazione di condizioni per l'esecuzione dei test; gli artt. 6 e 7 descrivono la procedura di preparazione ed esecuzione dei test. Infine, l'art. 8 affronta la gestione dell'esito della valutazione e le prescrizioni per l'utilizzo dell'oggetto dell'affidamento.

Inoltre, affronta la materia delle attività di verifica e di ispezione, che hanno lo scopo di accertare, nell'ambito di quanto previsto dal decreto, l'adempimento da parte dei soggetti inclusi nel perimetro dei seguenti obblighi:

a) predisposizione, aggiornamento e trasmissione dell'elenco delle reti, dei sistemi informativi e dei servizi informatici ai sensi dell'art. 1, comma 2, lettera b) del DL 105/2019;
b) notifica al CSIRT Italia degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici nei termini e con le modalità previste dal Decreto del Presidente del Consiglio dei Ministri di cui all'art. 1, comma 3, lettera a) del DL;
c) adozione delle misure di sicurezza di cui all'art. 1, comma 3, lettera b), del DL, nei termini e con le modalità previste dal relativo decreto attuativo;
d) comunicazione al CVCN di cui all'art. 1 comma 6, lettera a), del DL, nei termini e con le modalità previste dal presente Decreto;
e) impiego di prodotti e servizi sulle reti, sui sistemi informativi e per l'espletamento dei servizi informatici in conformità alle condizioni e con superamento dei test imposti dal CVCN ai sensi dell'art. 1, comma 6, lettera a), del DL;
f) collaborazione per l'effettuazione delle attività di test da parte dei soggetti ai sensi dell'art. 1, comma 6, lettera b), del DL;
g) osservanza delle prescrizioni formulate dalle Autorità competenti ai sensi dell'art. 1, comma 6, lettera c), del decreto-legge, all'esito delle attività di ispezione e verifica;
h) osservanza delle prescrizioni di utilizzo fornite dal CVCN al soggetto ai sensi dell'articolo 1, comma 7, lettera b), del DL.

Inoltre, il DPR entra nel merito delle modalità con cui le attività di verifica e ispezione devono essere eseguite (rispettivamente, art. 17 Attività di verifica e art. 18 Attività di ispezione).

2.5.6 DPCM 15 giugno 2021 (DPCM III)

Il DPCM del 15 giugno 2021 (DPCM III) [2.11] individua le categorie di beni, sistemi e servizi ICT destinati a essere impiegati sulle reti, sui sistemi informativi e per l'espletamento dei servizi informatici all'interno del PSNC, per i quali i soggetti in questo inseriti devono effettuare la comunicazione al CVCN di avvio della procedura di procurement. Corrisponde al Decreto che definisce quali tipologie di beni e servizi ICT (elenco nell'allegato 1 del Decreto) debbano essere sottoposti a procedure di verifica e ispezione previste dal DPR 54/2021.

2.5.7 DPCM 92/2022

Il DPCM 92/2022 [2.30] costituisce il regolamento in materia di accreditamento dei laboratori di prova (LAP) e di raccordi tra CVCN, LAP e CV del Ministero dell'Interno e del Ministero della Difesa. Nello specifico, definisce:

a) le procedure, le modalità e i termini da seguire per l'accreditamento dei CV e dei LAP, ciascuno nell'ambito delle rispettive competenze, in ordine all'esecuzione dei test, secondo le pertinenti modalità;
b) le procedure, le modalità e i termini da seguire in ordine alla gestione dei raccordi del CVCN con i LAP e i CV, anche al fine di assicurare il coordinamento delle rispettive attività e perseguire la convergenza e la non duplicazione delle valutazioni in presenza di medesime condizioni e livelli di rischio.

Il DPCM individua il CVCN come l'organismo di accreditamento dei LAP e dei CV, operando in conformità ai requisiti della norma tecnica (standard) UNI CEI EN ISO/IEC 17011.
In particolare, al CVCN vengono attribuiti i seguenti compiti:

a) accredita i LAP in possesso dei requisiti richiesti (artt. 8, 9, 10, 11 e 12) e i CV (art. 20);
b) intraprende iniziative al fine di garantire il mantenimento del livello di qualità dei LAP e la corretta attuazione delle determinazioni tecniche, delle specifiche tecniche e della redazione dei rapporti di prova;
c) stabilisce le metodologie di test;
d) vigila sull'attività dei LAP nel corso delle attività di test effettuando verifiche intermedie o a campione per la verifica del mantenimento dei requisiti di accreditamento (artt. 14, 15 e 16);
e) adotta specifiche determinazioni tecniche, assicurandone, nell'ambito delle proprie competenze, il rispetto e curandone l'aggiornamento. In particolare, tali determinazioni definiscono:
   1) i requisiti tecnici e logistici, tra cui quelli relativi alla dotazione strumentale per l'esecuzione dei test e alla protezione degli ambienti di test;
   2) le specifiche misure di sicurezza informatica;
   3) i requisiti di competenza ed esperienza necessari per l'accreditamento dei LAP, ivi comprese le modalità di redazione del curriculum professionale da presentare nella domanda di accreditamento;
   4) le aree di accreditamento;
   5) i test da eseguire;
   6) le attività relative all'esecuzione dei test soggette al divieto di divulgazione;
   7) le modalità di notifica delle limitazioni di operatività superiori a 24 ore;
   8) le modalità tecniche per l'applicazione dei raccordi tra il CVCN e i CV, concordandoli con questi ultimi per gli aspetti di loro competenza;
   9) le modalità esecutive delle comunicazioni con i LAP e i termini tecnici e organizzativi mediante i quali i raccordi trovano effettiva applicazione;
f) cura i raccordi con i LAP e i CV (art. 21), anche al fine di assicurare il coordinamento delle rispettive attività e perseguire la convergenza e la non duplicazione delle valutazioni in presenza di medesime condizioni e livelli di rischio;
g) redige e aggiorna periodicamente la lista dei beni, sistemi e servizi ICT oggetto di valutazione, per i quali sia stato emesso un rapporto di prova;

h) gestisce la piattaforma informatica per la conservazione e condivisione:
   1) di un elenco dei LAP contenente il nominativo del responsabile del laboratorio di prova, del responsabile del sistema di gestione per la qualità e del responsabile per i rapporti con il CVCN, nonché la durata e l'area dell'accreditamento;
   2) della documentazione di sintesi relativa ai rapporti di prova.

Infine, il CVCN, i CV e i LAP, al verificarsi di un incidente sulle reti, sui sistemi informativi e sui servizi informatici di pertinenza deputati allo svolgimento delle funzioni oggetto dell'accreditamento, in termini di compromissione della integrità o riservatezza dei dati e delle informazioni trattati, sono tenuti alla notifica al CSIRT Italia secondo le modalità indicate dal CSIRT stesso, entro il termine di 6 ore dal momento in cui sono venuti a conoscenza dell'incidente (art. 22).

2.5.8 DL 115/2022, art. 37

Il DL 115/2022, cosiddetto Decreto Aiuti bis – recante disposizioni a sostegno di famiglie e imprese per contrastare l'emergenza idrica, energetica ed economica – all'art. 37 contiene disposizioni in materia di cybersecurity. Nello specifico, interviene sul DL 174/2015 convertito, con modificazioni, dalla Legge 198/2015, aggiungendo l'art. 7-ter "Misure di intelligence di contrasto in ambito cibernetico".
Prevede che il Presidente del Consiglio dei Ministri, acquisito il parere del CISR e sentito il COPASIR possa emanare disposizioni per l'adozione di misure di intelligence di contrasto in ambito cibernetico, in situazioni di crisi o di emergenza a fronte di minacce che coinvolgono aspetti di sicurezza nazionale e non siano fronteggiabili solo con azioni di resilienza. Tali disposizioni sono adottate con la cooperazione del Ministero della Difesa e facendo ricorso alle garanzie funzionali, di cui all'art. 17 della Legge 124/2007 (in materia di non punibilità del personale dei servizi che ponga in essere condotte previste dalla legge come reato, legittimamente autorizzate di volta in volta in quanto indispensabili alle finalità istituzionali di tali servizi e proporzionali allo scopo, nel rispetto di limiti elencati dalla legge). Queste disposizioni disciplinano il procedimento di autorizzazione, le caratteristiche e i contenuti generali delle misure che possono essere autorizzate in rapporto al rischio per gli interessi nazionali coinvolti, secondo criteri di necessità e proporzionalità. L'autorizzazione è disposta sulla base di una valutazione volta a escludere, alla luce delle più aggiornate cognizioni informatiche, fatti salvi i fattori imprevisti e imprevedibili, la lesione dell'integrità fisica, la personalità individuale, la libertà personale, morale, la salute o l'incolumità di una o più persone.
Le misure di contrasto in ambito cibernetico autorizzate sono attuate dall'Agenzia Informazioni e Sicurezza Esterna (AISE) e l'Agenzia Informazioni e Sicurezza Interna (AISI), con il coordinamento del Dipartimento delle Informazioni per la Sicurezza (DIS), ferme restando le competenze del Ministero della Difesa. Il DIS assicura il coordinamento delle attività.
Sono inoltre contenute norme a tutela del personale impiegato nelle operazioni: al personale delle Forze Armate impiegato nell'attuazione delle attività di cui al presente articolo si applicano le disposizioni di cui all'art. 19 della Legge 145/2016 (Disposizioni in materia penale per il corpo militare impiegato in missioni internazionali) e, ove ne ricorrano i presupposti, dell'art. 17, comma 7, della Legge 124/2007 (in materia di garanzie funzionali).
Il Parlamento manterrà un ruolo di controllo: il Presidente del Consiglio dei Ministri informerà infatti il COPASIR sulle operazioni svolte entro 30 giorni dalla conclusione delle stesse.

Il COPASIR, inoltre, trascorsi 24 mesi dalla data di entrata in vigore della Legge, dovrà trasmettere alle Camere una relazione sull'efficacia delle norme contenute nell'articolo in oggetto.

2.5.9 Il Cyber Resilience Act: nuove prospettive per l'accreditamento

Nell'ambito del discorso sullo "Stato dell'Unione 2022", la Presidente della Commissione europea Ursula von der Leyen ha annunciato la presentazione del cosiddetto **"Cyber Resilience Act", una proposta di Regolamento UE in materia di sicurezza dei prodotti con elementi digitali (software o hardware)** il cui uso previsto (o ragionevolmente prevedibile) richiede una connessione di dati (diretta o indiretta) a un dispositivo o a una rete. La proposta di Regolamento si colloca nel solco degli altri provvedimenti europei adottati in materia di sicurezza digitale (su tutti il Cybersecurity Act) e si pone l'obiettivo di proteggere i consumatori e le imprese da prodotti con caratteristiche di sicurezza inadeguate.
Sono quindi introdotte norme per l'immissione sul mercato di prodotti con elementi digitali al fine di garantirne la cybersecurity. Sono altresì disciplinati: i requisiti essenziali per la progettazione, lo sviluppo e la fabbricazione di prodotti con elementi digitali e obblighi per gli operatori economici in relazione a tali prodotti; i requisiti essenziali per i processi di gestione delle vulnerabilità messi in atto dai fabbricanti per garantire la cybersecurity dei prodotti con elementi digitali durante l'intero ciclo di vita e obblighi per gli operatori economici in relazione a tali processi. Sono infine contenute norme in materia di vigilanza del mercato e applicazione.
La proposta di Regolamento prevede che ciascuno Stato notifichi alla Commissione e agli Stati membri – per il tramite del portale NANDO (New Approach Notified and Designated Organisations) – gli organismi di valutazione della conformità autorizzati a svolgere le proprie attività. Al fine di garantire il possesso dei requisiti previsti dal Regolamento da parte degli organismi e di prevedere il loro inserimento nel portale, è disposta l'istituzione di un'Autorità di notifica in ciascun Paese. L'Autorità si occuperà inoltre delle attività di monitoraggio sugli organismi di valutazione, con la facoltà di delegare tale funzione e quella di valutazione all'Ente unico di accreditamento, Accredia per l'Italia. A monte della procedura di notifica, vi è la presentazione, da parte dell'organismo di valutazione della conformità, di un'apposita istanza, corredata da una descrizione delle attività e delle procedure di valutazione della conformità; dall'elenco dei prodotti per i quali tale organismo dichiara di essere competente; da un certificato di accreditamento, se esistente, rilasciato da un organismo nazionale di accreditamento che attesti che l'organismo di valutazione della conformità soddisfa le prescrizioni regolamentari. Se l'organismo non è in grado di fornire un certificato di accreditamento, esso fornisce all'Autorità di notifica tutte le prove documentali necessarie per la verifica, il riconoscimento e il monitoraggio periodico della sua conformità ai requisiti previsti dalle disposizioni europee. L'organismo potrà inoltre svolgere attività di organismo notificato (Notified Body) solo se la Commissione o uno Stato membro non solleveranno obiezioni nelle due settimane successive alla notifica (se in possesso di un accreditamento) o nei due mesi successivi (in assenza di accreditamento). Si noti come, coerentemente con il Cybersecurity Act, la proposta di Regolamento effettui una distinzione tra le diverse tipologie di prodotti in base al rischio per la collettività che potrebbe derivare da un attacco cyber. Nello specifico, si fa riferimento a prodotti "critici", distinti in due differenti classi: classe I e classe II (prodotti maggiormente critici). Per l'immissione nel mercato dei prodotti di classe I e II non basterà una autodichiarazione di conformità, come per le altre categorie di prodotti, ma il produttore dovrà assicurare il rispetto di elevati standard di qualità, avvalendosi di organismi di valutazione della conformità notificati.

2.6 Regolamento CE 765/2008 relativo all'accreditamento

L'accreditamento, in base al Regolamento CE 765/2008, è una forma indipendente e autorevole di attestazione dell'imparzialità, competenza e adeguatezza degli organismi di valutazione della conformità (organismi di certificazione, ispezione, verifica e validazione, laboratori di prova, medici e di taratura, produttori di materiali di riferimento, organizzatori di prove valutative interlaboratorio, biobanche).
L'attività di accreditamento è disciplinata a livello europeo e internazionale, rispettivamente, dal Regolamento CE 765/2008 [2.26] e dalla norma tecnica ISO/IEC 17011, e in Italia è svolta da Accredia, l'Ente unico nazionale designato dal Governo. Nello specifico, secondo il Regolamento, gli organismi nazionali di accreditamento si sottopongono a una valutazione inter pares disposta da European Accreditation (EA) l'infrastruttura europea di accreditamento riconosciuta dalla Commissione.
La valutazione è effettuata sulla base di criteri e procedure validi e trasparenti. I requisiti che gli organismi di accreditamento nazionali devono soddisfare sono:

- essere organizzati in modo che ne sia garantita l'indipendenza dagli organismi di valutazione della conformità da essi valutati, siano liberi da pressioni commerciali e non entrino in conflitto d'interesse con gli organismi di valutazione della conformità;
- essere organizzati e gestiti in modo che sia salvaguardata l'obiettività e l'imparzialità delle loro attività;
- operare in modo che ogni decisione riguardante l'attestazione di competenza sia presa da persone competenti diverse da quelle che hanno effettuato la valutazione;
- adottare disposizioni atte a salvaguardare la riservatezza delle informazioni ottenute;
- individuare le attività di valutazione della conformità per le quali sono competenti a effettuare l'accreditamento, rinviando, se del caso, alle pertinenti legislazioni e norme comunitarie o nazionali;
- istituire le procedure necessarie per assicurare l'efficienza della gestione e l'adeguatezza dei controlli interni;
- disporre di un numero di dipendenti competenti sufficiente per l'esecuzione adeguata dei loro compiti;
- documentare le funzioni, le responsabilità e i poteri del personale che potrebbe influenzare la qualità della valutazione e dell'attestazione di competenza;
- istituire, applicare e aggiornare le procedure per controllare le prestazioni e la competenza del personale;
- verificare che le valutazioni della conformità siano eseguite in modo adeguato, evitando oneri

inutili per le imprese e tenendo debitamente conto delle dimensioni, del settore e della struttura delle imprese, del grado di complessità della tecnologia dei prodotti e del carattere di massa o seriale del processo di produzione;

- pubblicare annualmente resoconti oggetto di revisione contabile, in conformità ai principi di contabilità universalmente accettati.

La valutazione inter pares accerta, quindi, che gli organismi nazionali di accreditamento soddisfino le condizioni del Regolamento e i risultati della valutazione sono pubblicati e comunicati da EA.

2.7 La norma ISO/IEC 17011

La norma tecnica ISO/IEC 17011 disciplina le attività degli Enti di accreditamento in tutto il mondo, a garanzia della competenza, dell'indipendenza e dell'imparzialità della loro attività di valutazione [2.31]. Si applica anche agli Enti di accreditamento che operano al di fuori dell'Europa, che non hanno come riferimento il Regolamento UE 765/2008. La norma pone l'accento su due aspetti importanti della certificazione e dell'accreditamento:

- *Assess competence*, attività eseguita dagli Enti di accreditamento al fine di valutare le competenze degli organismi di valutazione della conformità (organismi e laboratori);

- *Assess conformity*, attività eseguita dagli organismi (di certificazione, ispezione, verifica e validazione) per valutare la conformità di prodotti, servizi e fornitori a specifiche e/o requisiti.

Per svolgere l'attività di assess competence, l'Ente di accreditamento deve rispettare determinati requisiti della norma ISO/IEC 17011; in sintesi:

- *Responsabilità legale*: avere uno status giuridico riconosciuto;

- *Struttura e organizzazione*: dare credibilità ai propri accreditamenti ed essere responsabile delle proprie decisioni in materia di accreditamento, tra cui la concessione, il mantenimento, l'estensione, la riduzione, la sospensione e la revoca;

- *Imparzialità*: essere organizzato e gestito in modo da salvaguardare l'obiettività e l'imparzialità delle sue attività e garantire che ogni decisione sull'accreditamento sia assunta da persone o comitati competenti, diversi da quelli che hanno effettuato la valutazione;

- *Confidenzialità*: salvaguardare la riservatezza delle informazioni ottenute nel corso delle attività di accreditamento a tutti i livelli operativi e decisionali, compresi i comitati e gli organismi esterni o le persone che agiscono per suo conto;

- *Responsabilità e finanziamento*: avere la capacità di coprire le passività derivanti dalle sue attività e disporre di risorse finanziarie, comprovate da registri e/o documenti, necessarie per lo svolgimento delle proprie attività;

- *Attività di accreditamento*: descrivere le proprie attività di accreditamento, facendo riferimento a standard internazionali, guide o altri documenti normativi. Inoltre, stabilisce le procedure per estendere le proprie attività e per rispondere alle richieste delle parti interessate, avendo l'obbligo di assicurare che i documenti prodotti siano stati formulati da comitati o persone in possesso delle necessarie competenze e, se del caso, con la partecipazione delle parti interessate;

- *Gestione*: stabilire, attuare e mantenere un sistema di gestione e migliorarne continuamente l'efficacia, in conformità ai requisiti della norma ISO/IEC 17011;

- *Risorse umane*: avere un numero sufficiente di personale competente (interno, esterno, temporaneo o permanente, a tempo pieno o parziale) in possesso dell'istruzione, della formazione, delle conoscenze tecniche, delle capacità e dell'esperienza necessarie per gestire il tipo, la gamma e il volume di lavoro richiesto. Inoltre, deve garantire l'esecuzione soddisfacente della valutazione e del processo decisionale di accreditamento, stabilendo procedure per il monitoraggio delle prestazioni e delle competenze del personale coinvolto;

- *Processo di accreditamento*: offrire una descrizione dettagliata delle procedure che un organismo di valutazione della conformità deve eseguire per richiedere e conseguire l'accreditamento per un determinato prodotto o servizio;

- *Responsabilità dell'organismo di accreditamento e dell'organismo di valutazione della conformità*: obblighi che un organismo o laboratorio si impegna a soddisfare costantemente verso l'Ente di accreditamento, come rispettare i requisiti applicabili alle aree in cui l'accreditamento è richiesto o concesso, e l'insieme degli obblighi dell'organismo di accreditamento verso gli organismi e laboratori.

L'ultima versione del 2017 della norma ISO/IEC 17011 amplia il perimetro d'azione degli organismi di accreditamento, che includono le attività di *testing, calibration, inspection, certification of management systems, persons, products, processes and services, provision of proficiency testing, production of reference materials, validation and verification*.

2.8 Norme tecniche e certificazioni

2.8.1 La norma UNI CEI EN ISO/IEC 27001

La norma tecnica UNI CEI EN ISO/IEC 27001 riguarda i sistemi di gestione per la sicurezza delle informazioni [2.27]. Come passaggio base, richiede l'analisi del contesto esterno e interno, al fine di individuare le minacce, le vulnerabilità, ma anche le opportunità e i punti di forza esistenti. Attraverso l'analisi vengono acquisiti elementi utili a indirizzare efficacemente le attività di prevenzione e protezione dalle minacce che riguardano sia la sicurezza delle informazioni, sia il transito e l'elaborazione delle informazioni nel cosiddetto cyberspazio. Il secondo passaggio è l'analisi dei processi e la mappatura dell'infrastruttura adottata per supportare i processi medesimi. Queste informazioni, correlate alla conoscenza di pericoli e minacce, saranno alla base dei processi di valutazione dei rischi e di analisi per la continuità operativa, che per un'organizzazione operante nel mercato attuale significa capacità di sopravvivenza a fronte dei molteplici incidenti informatici e di sicurezza oggi ipotizzabili (si pensi agli attacchi di tipo ransomware).

Definiti i rischi e i beni dell'organizzazione che possono essere esposti e/o comunque impattati dai relativi eventi, si potranno progettare e applicare le misure organizzative e/o tecniche necessarie a mitigare tali rischi, dette anche "controlli operativi". L'esistenza di tali rischi sarà intesa più come elemento di base per lo sviluppo di un percorso ottimale, per tenere sotto controllo l'organizzazione, piuttosto che come variabile negativa da ridurre a zero (cosa di per sé impossibile) magari rinunciando a delle opportunità di crescita e di affari. Questo approccio richiede una continua formazione delle risorse umane, per adottare i comportamenti più adeguati e per far sì che i controlli operativi continuino a operare con la migliore efficienza ed efficacia, nel mitigare i rischi di cybersecurity. Occorrono addestramento e creazione di consapevolezza, su motivazioni e obiettivi, nonché sulla conoscenza dei pericoli, delle minacce e della relativa gestione. Alla base rimane la certezza che nessun rischio può essere azzerato, al limite trasferito attraverso strumenti assicurativi. Inoltre, nulla rimane invariato nel tempo, pertanto le analisi di scenario (contesto esterno e interno) dei rischi e degli impatti sui processi in termini di operatività aziendale, non ultimo di continuità operativa, dovranno essere costantemente aggiornate. La norma implica, inoltre, un'adeguata allocazione delle responsabilità e la creazione di una reportistica interna per dare evidenza del corretto funzionamento dei processi e controlli operativi sviluppati per proteggerli. Occorre inoltre che le persone coinvolte, a tutti i livelli, vengano riconosciute dall'organizzazione e, se del caso, supportate dall'Alta Direzione. Applicando l'approccio iterativo del ciclo di Deming, richiede anche una supervisione indipendente sulle attività di progettazione, pianificazione, allocazione di responsabilità e risorse, nonché esecuzione, misurazione e adeguamento dei processi e dei controlli operativi. Questo processo, che prende il nome di Auditing Interno, consente alle organizzazioni di rilevare tempestivamente le anomalie presenti tra la progettazione organizzativa e lo svolgimento effettivo delle diverse attività che costituiscono i processi aziendali. La programmazione e pianificazione degli Audit Interni deve prendere in considerazione i processi più rischiosi, attraverso un campionamento mirato e specifico, in parte basato anche sulla casualità, senza dimenticare il raffronto con l'analisi di contesto. Con le informazioni derivanti dal monitoraggio continuo, frutto del funzionamento dei controlli operativi (misure organizzative e tecniche per il mantenimento sotto controllo dei processi e dello stesso sistema di gestione) e del monitoraggio ad hoc svolto tramite gli Audit Interni, l'Alta Direzione ottiene gli elementi per prendere decisioni operative in specifici "momenti di riflessione" (Riesame della Direzione) con una frequenza di aggiornamento ritenuta adeguata. Dal Riesame sul raggiungimento degli obiettivi e dei target, sull'esigenza di risorse o di aggiornamento di alcuni processi, di approfondimento di specifici rischi e dei relativi controlli operativi, derivano le decisioni di governo aziendale.La norma ISO/IEC 27001 prevede l'analisi di uno specifico allegato, che richiama 14 aree di attenzione per il possibile sviluppo dei controlli operativi. Nel dettaglio[11]:

- Politiche di sicurezza;
- Organizzazione della sicurezza;
- Sicurezza delle risorse umane;
- Gestione degli asset;
- Controllo degli accessi;
- Crittografia;

[11] A ottobre 2022 è stata pubblicata la nuova versione della norma ISO/IEC 27001 che contiene una diversa classificazione degli stessi controlli; alcuni sono stati raggruppati, altri inseriti ex novo. Sono state inoltre inserite precisazioni e integrazioni che non hanno tuttavia cambiato la struttura sistemica.

- Sicurezza fisica e ambientale;
- Sicurezza delle attività operative;
- Sicurezza delle comunicazioni;
- Acquisizione, sviluppo e manutenzione dei sistemi;
- Relazione con i fornitori;
- Gestione degli incidenti relativi alla sicurezza delle informazioni;
- Continuità operativa;
- Conformità alla normativa.

La definizione di quali controlli adottare tra quelli indicati e di quali ulteriori sviluppare, è responsabilità dell'organizzazione. Tale scelta è una diretta conseguenza della valutazione dei rischi e della *Business Impact Analysis* (BIA) che è una forma di valutazione dell'impatto dei diversi processi nel raggiungimento degli obiettivi aziendali. Accredia, l'Ente italiano di accreditamento, nella gestione del proprio schema di accreditamento per lo *schema sistemi di gestione per la sicurezza delle informazioni* (ISMS - Information Security Management System) adotta dei particolari punti di attenzione. In fase di valutazione preliminare, quando viene ricevuta la domanda di accreditamento da parte di un organismo di certificazione, innanzi tutto viene valutato se lo stesso organismo richiede di operare sull'intero campo di applicazione dello schema, oppure se indica alcune aree tecniche specifiche, di propria specializzazione. Di solito, gli organismi chiedono di operare nell'area tecnica più ampia possibile, abbracciando ambiti anche molto diversi, pertanto è cura di Accredia verificare se e come l'organismo abbia le competenze per operare in tali aree. Si tratta, ad esempio, delle aree industriali, oppure di servizi, che possono andare da quelli sociali e/o sanitari a quelli di trasporto o di comunicazione o di erogazione di servizi fiduciari (cosiddetti trusted). Si può trattare di servizi cloud o di gestione di infrastrutture in ambito Transizione 4.0, ma anche di servizi e infrastrutture bancarie, assicurative o finanziarie, oppure della gestione di infrastrutture di pubblico interesse, come la distribuzione di acqua o gas o di energia, ma anche di produzione di tali beni. Queste aree, citate a solo titolo di esempio, richiedono da parte dell'organismo una competenza che può avere sfumature differenziate. Si passa dalla competenza sugli aspetti legali e normativi che impattano sugli stessi ISMS a quelli di tipo più squisitamente tecnico, legati alle cosiddette "buone pratiche" definite a livello industriale e, magari, anche normate in documenti guida della serie 27XXX. Talora questi documenti possono affiancare la norma UNI CEI EN ISO/IEC 27001, talora sono semplici guide, dalle quali è possibile trarre spunto come pratiche validate oppure per la progettazione di quei controlli operativi atti a mitigare il rischio. Dopo le valutazioni sulle competenze attese da parte delle risorse umane dell'organismo di certificazione (addetti alle attività commerciali, responsabili di schema, responsabili del programma di audit, auditor e decisori) Accredia si concentra su altri elementi portanti:

- Viene richiesto all'organismo di produrre la documentazione di sistema, che funge da progetto della propria attività di certificatori e prevede uno schema di certificazione specifico, necessario per comunicare al mercato delle organizzazioni interessate alla certificazione quali siano le regole da applicare. Include un documento con le modalità di qualifica degli auditor e l'elenco e curricula degli stessi operatori della certificazione: auditor e decisori.

- Viene definito l'iter operativo del processo di certificazione: cosa verificare presso la sede dell'organismo e quali attività svolgere in campo (cosiddette verifiche in accompagnamenti o *witness*). Il progetto viene definito con criterio presso la sede dell'organismo.

- Gli ispettori di Accredia valutano le competenze operative del personale dell'organismo addetto alle verifiche presso la sede delle organizzazioni da certificare. La scelta delle organizzazioni ove svolgere le verifiche in accompagnamento discende dalla valutazione dei rischi svolta dal funzionario tecnico di Accredia responsabile della pratica di accreditamento. Vengono infatti selezionate le aree tecniche a maggiore criticità, ove verificare de visu la reale competenza operativa dell'organismo che richiede l'accreditamento.

2.8.2 Framework Nazionale per la Cybersecurity e la Data Protection

Il Framework Nazionale per la Cybersecurity e la Data Protection è inteso a supportare le aziende nella individuazione delle vulnerabilità del loro sistema di trattamento delle informazioni e procedere, se è il caso, a rafforzarlo minimizzando il rischio di incidenti e di danni ingenti [2.28]. Basato sul *Cybersecurity Framework for Critical Infrastructur*e creato dal NIST[12], si sviluppa in maniera gerarchica in *function, category e subcategory*. Tali elementi sono generali e indipendenti rispetto al settore produttivo, alla tipologia degli impiegati, alla dimensione e alla dislocazione sul territorio dell'organizzazione.

Le function sono 5:

- **Identify**: associata alla comprensione del contesto aziendale, degli asset che supportano i processi critici di business e dei relativi rischi associati;

- **Protect**: legata all'implementazione di misure volte alla protezione dei processi di business e degli asset aziendali;

- **Detect**: finalizzata alla definizione e attuazione delle attività appropriate per identificare tempestivamente incidenti di sicurezza informatica;

- **Respond**: legata alla definizione e attuazione delle opportune attività per intervenire quando un incidente di sicurezza informatica sia stato rilevato;

- **Recover**: associata alla definizione e attuazione delle attività per la gestione dei piani e delle attività per il ripristino dei processi e dei servizi impattati da un incidente.

A ogni *function* corrispondono più *category* e *subcategory* riguardanti le attività abilitanti, quali processi e tecnologie, da mettere in campo per gestire i vari aspetti della sicurezza dell'organizzazione, quali aspetti di governance, valutazione e gestione dei rischi, processi di identificazione e gestione delle minacce, ecc. L'applicazione del Framework a un'organizzazione richiede una fase iniziale di contestualizzazione, nella quale l'organizzazione seleziona le subcategory che meglio colgono la strategia di gestione della cybersecurity che la stessa intende adottare. In questa fase è necessario tenere conto di eventuali requisiti imposti da regolamenti e leggi, o criteri suggeriti da *best practice* che si intendono adottare. Per ogni subcategory selezionata devono essere definiti una priorità di implementazione e un set di controlli che individueranno le soluzioni con cui si intende implementare quella specifica subcategory.

[12] *https://www.nist.gov/cyberframework*

Grazie a queste proprietà, il Framework può essere adattato in modo flessibile alle esigenze e alle caratteristiche di realtà organizzative molto diverse tra loro. I contenuti dell'allegato B del DPCM 81/2021 (DPCM II) sono basati in toto sulla struttura del Framework.

2.8.3 Common Criteria (norma ISO/IEC 15408)

***I Common Criteria for Information Technology Security Evaluation* (noti come *Common Criteria* o CC) sono una norma tecnica internazionale (ISO/IEC 15408) per la certificazione della sicurezza informatica dei prodotti hardware e software** [2.29]. In Italia le certificazioni Common Criteria e l'accreditamento dei relativi LVS sono stati gestiti da OCSI sino alla creazione dell'ACN. La norma comprende cataloghi di requisiti funzionali (CC parte 2) e di requisiti di sicurezza (CC parte 3), insieme a istruzioni su come costruire specifiche di sicurezza (chiamate anche "Security Target", cfr. CC parte 1) e condurre valutazioni di sicurezza indipendenti basate su questi requisiti (CEM). I Common Criteria prevedono che produttori di apparecchiature hardware o sviluppatori di prodotti software possano specificare i loro requisiti funzionali e di controllo della sicurezza (rispettivamente *Security Functional Requirements* - SFR, e *Security Assurance Requirements* - SAR) in un *Security Target* - ST, che possono essere tratti dai *Protection Profiles* (PP) definiti nell'ambito dei CC.
I laboratori di prova effettuano le valutazioni e le verifiche sui prodotti per determinare se soddisfino effettivamente le dichiarazioni. Le verifiche possono essere effettuate secondo livelli crescenti di complessità, individuati da numeri, da 1 a 7: un prodotto con verifica EAL1 (*Evaluation Assurance Level*) è stato sottoposto all'insieme minimo di verifiche stabilito dallo standard, mentre un prodotto certificato EAL7 è stato sottoposto a verifica in accordo con l'insieme delle metodologie che consentono il massimo dettaglio e che, di conseguenza, richiedono un maggior quantitativo di tempo e risorse.
I Common Criteria garantiscono che il processo di specificazione, implementazione e valutazione di un prodotto informatico sia stato condotto in modo rigoroso, standard e ripetibile rispetto alle funzionalità di sicurezza prescritte per quella tipologia di prodotto, commisurate all'ambiente di utilizzo e al relativo rischio previsto. I prodotti valutati secondo i Common Criteria sono pubblicati nel portale ufficiale[13] , che comprende, ad esempio, sistemi operativi, sistemi di controllo degli accessi, database e sistemi di gestione delle chiavi.
Il Common Criteria Recognition Arrangement (CCRA) è un accordo tra i partecipanti agli schemi di valutazione e altre organizzazioni interessate. I partecipanti agli schemi assicurano che i prodotti siano valutati da laboratori autorizzati, competenti e indipendenti in base a standard comuni, in modo da determinare il soddisfacimento di particolari proprietà di sicurezza, con un certo grado di garanzia. I certificati risultanti possono essere riconosciuti da tutti i firmatari del CCRA: i partecipanti al CCRA riconoscono che il sistema di valutazione della nazione che ha rilasciato il certificato ha eseguito correttamente tutte le attività coinvolte nei processi CC e CCRA. Ciò non implica che il prodotto IT certificato soddisfi i requisiti di sicurezza di un'altra nazione partecipante alla CCRA. Per raggiungere questo obiettivo, i profili di protezione collaborativi (cPP) sono sviluppati da comunità tecniche internazionali composte da fornitori, laboratori di prova, nazioni CCRA e centri accademici. I cPP sono sviluppati con il coinvolgimento e l'approvazione di tutte le nazioni partecipanti alla CCRA. All'interno del CCRA, tutte le valutazioni che utilizzano un cPP sono riconosciute reciprocamente. In alcuni casi specifici, un cPP può raggiungere il livello di garanzia della valutazione EAL4. Le valutazioni non basate su un cPP sono riconosciute fino a EAL2.

[13] *https://www.commoncriteria.org*

Il CCRA prevede il riconoscimento reciproco tra gli schemi di valutazione per valutazioni fino a EAL1-2; in alcuni casi specifici, la valutazione cPP potrebbe raggiungere EAL4. Un elenco dei Certificate Authorizing Schemes ai sensi del CCRA è disponibile sul sito ufficiale, come pure l'elenco dei profili di protezione certificati, dei laboratori autorizzati e dei prodotti certificati. Parallelamente al CCRA, i Paesi europei coinvolti nel precedente schema ITSEC riconoscono EAL più elevati nell'ambito del cosiddetto SOG-IS European Mutual Recognition Agreement (SOG-IS MRA). Il SOG-IS MRA copre due domini tecnici: Smartcard & Similar Devices e Hardware Devices with Security Boxes, per i quali sono riconosciute valutazioni fino a EAL7. Le valutazioni al di fuori di questi domini tecnici sono riconosciute fino a EAL4. Il numero di Paesi europei che partecipano al SOG-IS MRA è pari a 10. Ciascuno di questi Paesi ha concesso la licenza a un certo numero di strutture di valutazione della sicurezza informatica (ITSEF) che eseguono le valutazioni. Un ITSEF può essere qualificato per "Tutti i prodotti" su EAL1-4, per "Smartcard e dispositivi simili" su EAL1-7, e/o per "Dispositivi hardware con box di sicurezza" su EAL1-7. L'elenco completo degli ITSEF è disponibile sul sito ufficiale. Il Common Criteria è spesso utilizzato come base per uno schema di certificazione guidato dal governo e, in genere, le valutazioni sono condotte per l'uso di agenzie governative e infrastrutture critiche.

Valutazione e governance

La governance complessiva dello schema Common Criteria è simile in entrambi gli accordi (CCRA e SOG-IS MRA). I certificati possono essere emessi in modo indipendente da uno qualsiasi degli *Schemi di Autorizzazione dei Certificati (Certificate Authorizing Schemes)*. Ciascuno di questi schemi ha riconosciuto diversi laboratori di valutazione, che effettuano le valutazioni effettive dei prodotti. Lo status di Schema di Autorizzazione dei Certificati si ottiene attraverso un processo di revisione paritaria per mezzo dei cosiddetti audit CB (*Certification Body - organismi di certificazione/validazione*). Gli audit CB di SOG-IS richiedono una verifica più approfondita rispetto agli audit CB eseguiti in CCRA, con una forte attenzione alle competenze tecniche sia del personale CB sia dei laboratori autorizzati dal CB.

Processo di certificazione

La valutazione serve a convalidare le affermazioni fatte su un prodotto. Per essere di utilità pratica, la valutazione deve verificare le caratteristiche di sicurezza del prodotto. Ciò avviene come segue:

1. Un Protection Profile può essere creato da una comunità di utenti, che identifica i requisiti di sicurezza per una classe di prodotti (per esempio, smart card utilizzate per fornire firme digitali o firewall di rete).
2. Il Protection Profile è certificato da un laboratorio di prova indipendente per assicurarsi che sia conforme a tutti i requisiti CC applicabili.
3. Un fornitore di prodotti sceglie di creare un prodotto conforme a uno o più PP e scrive un Security Target che spiega come i requisiti di sicurezza di questi PP sono soddisfatti dal prodotto. Se non esiste un PP per il tipo di prodotto, il fornitore può preparare direttamente il proprio Security Target.
4. Un laboratorio di valutazione riconosciuto e selezionato dal fornitore valuta il prodotto (TOE) rispetto al Security Target per assicurarsi che le affermazioni funzionali e di sicurezza fatte dal fornitore nella ST siano effettivamente valide. I risultati sono documentati in un Evaluation Technical Report (ETR).
5. Sulla base del rapporto di valutazione, il sistema di autorizzazione dei certificati che ha concesso la licenza al laboratorio convalida l'ETR e può rilasciare un certificato Common Criteria per il prodotto.

La certificazione può riguardare anche altri obiettivi contrattuali, talvolta definiti dal settore privato. A volte i fornitori di software o le industrie utilizzano il processo di certificazione per differenziare i loro prodotti dalla concorrenza.

I Common Criteria descrivono l'insieme delle azioni generali che i valutatori devono svolgere. La documentazione di supporto può essere definita per descrivere come vengono applicati i criteri e i metodi di valutazione nella valutazione di tecnologie specifiche. Tali documenti contribuiscono ad armonizzare gli approcci dei CB, sostituendo le molteplici interpretazioni individuali e forniscono quindi chiarezza a sviluppatori, valutatori e certificatori. La loro rilevanza e il loro utilizzo per particolari tecnologie sono approvati dal rispettivo Comitato di gestione (SOG-IS e/o CCRA) dopo la presentazione di un'adeguata motivazione. Esistono due classi di documentazione di supporto CC:

- "Documenti di supporto obbligatori" che devono essere applicati quando si valuta un prodotto che coinvolge una particolare tecnologia. Se la documentazione non viene applicata, il certificato non beneficerà del mutuo riconoscimento;

- "Documenti di supporto orientativi" contengono consigli più generali e buone pratiche.

Attualmente la maggior parte dei documenti tecnici di supporto CCRA è stata fornita alla comunità CCRA dal SOG-IS dopo un periodo di prova. I documenti di supporto del SOG-IS sono disponibili sul sito ufficiale. Tra gli esempi vi sono:

- i Meccanismi crittografici concordati del SOG-IS, che elencano i meccanismi crittografici concordati, in particolare per quanto riguarda la loro forza di sicurezza;

- il SOG-IS Joint Interpretation Working Group (JWIG) Minimum Site Requirements, che definisce una serie di requisiti minimi per la sicurezza del sito in cui viene sviluppata una smartcard e dispositivi simili. Questi requisiti sono applicabili da EAL3 in su, ma soprattutto per EAL4+ e superiori.

Durata della fase di valutazione
Una valutazione tipica può durare da 6 a 14 mesi. Il costo della valutazione dipende dalla complessità del prodotto, dalla maturità di sicurezza dello sviluppatore e dal livello di garanzia di valutazione desiderato. Gli EAL più elevati non comportano necessariamente valutazioni più lunghe, mentre la maturità complessiva dell'ecosistema è un fattore molto più importante. I profili di protezione e i documenti di supporto concordati da una comunità (sul modello del gruppo di esperti del Joint Interpretations Working Group del SOG-IS) contribuiscono a metodi di valutazione più pertinenti e a tempi più brevi. La maturità dello sviluppatore è un fattore chiave anche per quanto riguarda il tempo di esecuzione della valutazione: in caso di fallimento di un'unità di lavoro, lo sviluppatore può apportare correzioni e presentare di nuovo il prodotto al valutatore: CC non limita il numero di correzioni apportate durante una valutazione. Le valutazioni possono quindi essere influenzate da ritardi dovuti a un prodotto non sufficientemente corretto o a ritardi nella correzione del prodotto. Tutte le indicazioni precedenti riguardano solo le valutazioni di uno specifico Target Of Evaluation (TOE) rispetto a un Protection Profile (PP) esistente o non utilizzando alcun PP. Nel caso in cui sia necessario un nuovo PP, il processo di certificazione di tale PP dura generalmente meno di 3 mesi.

Sono obbligatori per le valutazioni Common Criteria di smartcard e dispositivi simili, compreso lo sviluppo del relativo software, ma possono essere verificati durante qualsiasi tipo di valutazione Common Criteria.

2.8.4 European Cybersecurity Skills Framework & Digital Education Action Plan

L'Europa è in ritardo nello sviluppo di un approccio globale per definire un insieme di ruoli e competenze rilevanti per il settore della cybersecurity, come descritto nel rapporto ENISA "Cybersecurity Skills Development in the EU"[14]. Sebbene la cybersecurity sia una sfida mondiale che riguarda tutti i Paesi, esistono molte differenze nel modo in cui viene affrontata da ogni Stato. Per questo motivo, i Framework nazionali esistenti in materia di cybersecurity risultano incompatibili o, più in generale, non adeguati alle esigenze, alle leggi e ai regolamenti europei. Lo sviluppo di un Framework europeo delle competenze in materia di sicurezza informatica che tenga conto delle esigenze dell'UE e di ciascuno dei suoi Stati membri è considerato un passo essenziale verso il futuro digitale dell'Europa. **Lo *European Cybersecurity Skills Framework* (ECSF)[15] 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, 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. Il 5 aprile 2022 è stata presentata al pubblico una versione consolidata della bozza dello ECSF. Di seguito si riportano i profili di competenza individuati nel draft:

- Chief Information Security Officer (CISO);
- Cyber Incident Responder;
- Cyber Legal, Policy & Compliance Officer;
- Cyber Threat Intelligence Specialist;
- Cybersecurity Architect;
- Cybersecurity Auditor;
- Cybersecurity Educator;
- Cybersecurity Implementer;
- Cybersecurity Researcher;
- Cybersecurity Risk Manager;
- Digital Forensics Investigator;
- Penetration Tester.

Nel contesto della carenza e del divario di competenze in materia di cybersecurity, in tutto il mondo, inclusa l'Europa, 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.

---

[14] *https://www.enisa.europa.eu/publications/the-status-of-cyber-security-education-in-the-european-union*
[15] *https://www.enisa.europa.eu/topics/cybersecurity-education/european-cybersecurity-skills-framework/ecsf-profiles-v-0-5-draft-release.pdf*

Esempi sono i programmi CyberChallenge.it[16], OlyCyber.it[17] e CyberTrials[18] promossi, nel contesto italiano, dal Cybersecurity National Lab[19] del CINI. Dal 2010, l'Agenda digitale europea della Commissione europea ha evidenziato la sfida della "mancanza di alfabetizzazione e competenze digitali" e che il loro potenziamento promuoverebbe l'occupazione nel settore generale delle ICT (compresa la sicurezza). Inoltre, è stato notato che la "carenza di competenze ICT" deve essere affrontata attraverso il coordinamento e un approccio congiunto degli Stati membri dell'UE. Obiettivi simili sono stati inseriti anche nel rinnovato Piano d'azione per l'istruzione digitale (2021-2027)[20]. Inoltre, per affrontare il crescente divario tra le capacità e le esigenze del mercato causato dalla rapida evoluzione della tecnologia, sono state lanciate iniziative come la Piattaforma europea per le competenze e l'occupazione digitale (Digital Skills and Jobs Platform)[21], che offre informazioni e risorse sulle competenze digitali.

2.8.5 International Information System Security Certification Consortium (ISC)2

Tra le organizzazioni mondiali specializzate nella formazione e nelle certificazioni per i professionisti della sicurezza informatica emerge, per dimensione del numero di partecipanti e il livello di qualità delle competenze certificate, l'International Information System Security Certification Consortium o (ISC)2[22]. (ISC)2 mantiene quello che prende il nome di Common Body of Knowledge per la sicurezza delle informazioni, ossia:

- **Certified Information Systems Security Professional (CISSP)** che racchiude le seguenti certificazioni:

  - Information Systems Security Architecture Professional (CISSP-ISSAP), che si concentra sugli aspetti architetturali della sicurezza delle informazioni. Le 6 aree coperte dalla certificazione sono:

    1. Identity and Access Management Architecture;
    2. Security Operations Architecture;
    3. Infrastructure Security;
    4. Architect for Governance, Compliance, and Risk Management;
    5. Security Architecture Modeling;
    6. Architect for Application Security.

  - Information Systems Security Engineering Professional (CISSP-ISSEP) che si focalizza sugli aspetti ingegneristici della sicurezza delle informazioni nel ciclo di vita dello sviluppo dei sistemi.

Le 5 aree coperte dalla certificazione sono:

1. Security Engineering Principles;
2. Risk Management;

---

[16] *https://cyberchallenge.it/*
[17] *https://olicyber.it/*
[18] *https://www.cybertrials.it/*
[19] *https://cybersecnatlab.it*
[20] *https://education.ec.europa.eu/focus-topics/digital-education/digital-education-action-plan*
[21] *https://digital-skills-jobs.europa.eu/en*
[22] *https://www.isc2.org/*

3. Security Planning, Design, and Implementation;
4. Secure Operations, Maintenance, and Disposal;
5. Secure Engineering Technical Management.

- Information Systems Security Management Professional (CISSP-ISSMP), improntata sugli aspetti gestionali della sicurezza delle informazioni. Le 6 aree coperte dalla certificazione sono:

1. Leadership and Business Management;
2. Systems Lifecycle Management;
3. Risk Management;
4. Threat Intelligence and Incident Management;
5. Contingency Management;
6. Law, Ethics, and Security Compliance Management.

- **Certified Secure Software Lifecycle Professional (CSSLP**) è una certificazione che si concentra sulla sicurezza delle applicazioni nell'ambito del ciclo di vita dello sviluppo del software (SDLC);

- **Certified Authorization Professional (CAP)** è una certificazione che verifica, convalida e certifica le competenze, l'esperienza e le metodologie di un individuo nella implementazione e nella gestione delle autorizzazioni per i sistemi informatici;

- **Certified Cloud Security Professional (CCSP)** è una certificazione di competenze e conoscenze tecniche avanzate per progettare, gestire e proteggere i dati, le applicazioni e l'infrastruttura nel cloud;

- **Systems Security Certified Practitioner (SSCP)** certifica le competenze e le conoscenze tecniche avanzate per implementare, monitorare e amministrare una infrastruttura IT;

- **Health Care Information Security and Privacy Practitioner (HCISPP**) è una certificazione che combina le competenze di cybersecurity con le migliori pratiche e tecniche di privacy, dimostrando le conoscenze e la capacità di implementare, gestire e valutare i controlli di sicurezza e privacy per proteggere le organizzazioni in ambito sanitario.

2.8.6 Altre certificazioni di competenza basate su norme tecniche CEN e UNI

2.8.6.1 La norma UNI 11506

Nel panorama delle certificazioni professionali in ambito ICT, si individuano le certificazioni delle figure professionali previste dalla norma tecnica UNI 11506 [2.34] e dalle norme cosiddette "multiparte", della serie UNI 11621 [2.33]. Lo standard UNI 11506 definisce i requisiti per la valutazione e la certificazione delle conoscenze, abilità, autonomia e responsabilità per i profili professionali ICT basati sul modello e-CF (UNI EN 16234-1) [2.35], indipendentemente dalle modalità lavorative e dalla tipologia del rapporto di lavoro, ossia i criteri generali delle figure professionali operanti nel settore dell'ICT, stabilendo i requisiti fondamentali per l'insieme di conoscenze, abilità e competenze che le contraddistinguono.

La norma definisce le modalità di certificazione rispetto alle norme della serie UNI 11621. I requisiti sono definiti, a partire dai compiti e attività specifiche e dall'identificazione dei relativi contenuti, in termini di conoscenze e abilità, anche al fine di identificarne chiaramente il livello di autonomia e responsabilità in coerenza con il Quadro Nazionale delle Qualificazioni (QNQ).
Inoltre i requisiti sono inoltre espressi in maniera tale da agevolare e contribuire a rendere omogenei e trasparenti, per quanto possibile, i relativi processi di valutazione della conformità.
Con l'uscita della versione 2021 della norma UNI 11506 e delle norme multiparte UNI 11621-X si è modificato in parte il panorama delle possibili definizioni/descrizioni delle figure professionali in ambito ICT. Le figure professionali sono classificate in base ai "ruoli" e ai parametri di *conoscenza*; *abilità* (capacità di applicare le conoscenze e di usare il know-how per portare a termine compiti e risolvere problemi); *autonomia e responsabilità* (capacità della persona di applicare le conoscenze e abilità in modo autonomo e responsabile).
La certificazione delle persone in base alle norme indicate avviene tramite processi svolti da organismi di certificazione accreditati da Accredia in conformità alla norma UNI CEI EN ISO/IEC 17024 [2.32], che disciplina il processo di valutazione di conformità di terza parte, proprio per le figure professionali. La certificazione accreditata, ai fini della validità rispetto alla Legge 4/2013, viene condotta sotto accreditamento per ogni specifica norma, come riportato anche nel D.Lgs 13/2013 [2.36]. Per i professionisti ICT, la certificazione rilasciata dagli organismi accreditati diventa un valore aggiunto per posizionarsi in un mercato sempre più competitivo, forti di un set di competenze, conoscenze e abilità che sono state verificate e attestate in maniera indipendente e imparziale. Tra queste, un professionista che opera in un'organizzazione pubblica o privata o come free lance, deve essere in grado di svolgere tutti i compiti necessari per gestire un'infrastruttura ICT, come garantire l'operatività delle infrastrutture, occuparsi della sicurezza delle informazioni, assicurare l'erogazione dei servizi offerti sul web.

2.8.6.2 Le norme per le competenze dei professionisti ICT

La norma UNI EN 16234-1 "e-Competence Framework (e-CF) - Framework comune europeo per i professionisti ICT in tutti i settori - Parte 1: Framework (modello di riferimento)" recepisce il modello europeo e-Competence Framework 4.0 (e-CF 4.0) contenente la definizione di diversi livelli di conoscenze, abilità, autonomia e responsabilità necessari per la predisposizione di profili ICT.
Al fine di evitare una proliferazione di profili, con relativa confusione sul mercato delle professionalità operanti nel settore ICT, il Comitato Europeo di Normazione (CEN) tramite il CWA 16458 [2.37] (pubblicata in Italia come UNI 11621 parte 1 e 2) ha proposto un modello di riferimento per la creazione dei profili (norma UNI 11621-1) e 23 profili professionali ICT (norma UNI 11621-2) definiti come profili di "seconda generazione". Il CWA è stato successivamente aggiornato con la definizione di 30 profili europei, mantenendo il riferimento al modello per la predisposizione dei profili professionali nella parte 2 del nuovo CWA. Il modello prevede la possibilità di creare profili definiti di "terza generazione". Sempre al fine di evitare frammentazione nella creazione dei profili ed al fine di supportare quanto richiesto dalla Legge 4/2013 in materia di creazione di norme tecniche UNI rispetto a specifiche professionalità non regolamentate, è nata la serie delle norme UNI 11621-X (riportate nei riferimenti normativi). La serie della **norma UNI 11621-X** per le professioni ICT, come già specificato nelle norme stesse, tratta anche le attività professionali regolamentate in ordini o collegi, di cui al DPR 137/2012, disciplinate nel DPR 328/2001 e successive modificazioni e integrazioni. Sempre basati sulla norma UNI CEI EN ISO/IEC 17024:2012, esistono degli schemi di

certificazione destinati alle figure professionali degli auditor e lead auditor per i sistemi di gestione. Tra questi, sono da menzionare le figure professionali dedicate ai sistemi di gestione per la sicurezza delle informazioni e cybersecurity, così come i sistemi per la gestione dei servizi informatici. A questi professionisti, certificati a fronte, rispettivamente, delle norme **ISO/IEC 27001** e la **ISO/IEC 20000-1**, viene richiesta anche la conoscenza dalla norma **UNI EN ISO 19011**, che è la Linee Guida dedicata allo svolgimento degli audit interni per i sistemi di gestione e introduce i principali requisiti fondanti di una cultura e di un approccio robusto al processo di auditing. Gli organismi di certificazione accreditati per tali schemi, possono inserire negli esami previsti per tali figure professionali, anche la conoscenza dei principali requisiti applicabili per gli audit di terza parte, sulla base di quanto indicato dalla UNI CEI EN ISO/IEC 17021-1, in particolare al § 9, sebbene questo sia un elemento che, ove necessario, diverrà oggetto di formazione e qualifica specifica da parte di ogni organismo, all'atto della qualifica dei propri auditor di terza parte. Il punto di forza di queste certificazioni è costituito dalla visione allargata che presuppone, da un lato l'elemento comune della cultura sistemica, quindi tipicamente del miglioramento continuo secondo le logiche HLS (High Level Structure) e, dall'altro, la competenza tecnica di schema.
Quest'ultima viene valutata rispetto alla conoscenza dei fondamentali per la sicurezza delle informazioni e cybersecurity (ISMS) e alla definizione degli strumenti gestionali per il buon governo dei processi che realizzano i servizi IT (ITSMS).
Infine, sempre sotto l'accreditamento di Accredia, per le competenze a livello di "utilizzatore dei computer" la Comunità europea ha sviluppato negli ultimi anni un quadro di riferimento, che a sua volta ha generato nel 2013 la base del modello DIGCOMP con DIGCOMP 1.0 e nel 2016 il DIGCOMP 2.0: The Digital Competence Framework for Citizens - The Conceptual Reference Model. La UE ha poi generato un documento condiviso da tutti gli Stati membri che è il riferimento unico per i cittadini, il DIGCOMP 2.1 che è l'evoluzione del quadro di riferimento per le competenze digitali e illustra 8 livelli di padronanza ed esempi di utilizzo applicati al settore dell'istruzione.

2.8.6.3 Metodi di valutazione applicabili per i professionisti ICT

Nell'apprendimento formale (scolastico e universitario), le metodologie e i soggetti che effettuano la valutazione sono stabiliti per via legislativa (per esempio esami di Stato, esami di maturità). Ciò non avviene in ambito non formale e informale. Per la valutazione della conformità relativa ai risultati dell'apprendimento non formale e informale, devono essere valutate in modo oggettivo e diretto le conoscenze, l'abilità, l'autonomia e la responsabilità. Per garantire l'efficacia della valutazione delle competenze occorre indicare una combinazione di più metodi di valutazione, tra i quali vanno indicati almeno i seguenti:

1) *analisi del curriculum vitae* integrato da documentazioni comprovanti le attività lavorative e formative dichiarate dal candidato (vedere punto A.2);
2) *esame scritto* per la valutazione delle conoscenze. Tale prova di esame può consistere in:
   - una prova con domande a risposta chiusa: per esempio, per ogni domanda vengono proposte almeno 4 risposte delle quali 1 sola è corretta (da escludere quelle del tipo "vero/falso); e/o
   - una prova con domande a risposta aperta: per esempio, per ciascuna domanda il candidato dovrà fornire una risposta appropriata.
3) *esame orale* necessario per approfondire eventuali incertezze riscontrate nelle prove scritte e/o per approfondire il livello delle conoscenze acquisite dal candidato.

Si riportano nel seguito altri possibili metodi che, in funzione delle specificità dell'attività professionale oggetto di normazione, possono essere inseriti o integrati nell'elenco precedente, (in particolare i punti da 4 a 6), al fine di rendere coerente l'insieme degli strumenti di valutazione con l'oggetto della stessa (ossia descrittori specificati al punto 5), tenendo comunque presente che ne potrebbero essere considerati anche altri:

4) *esame scritto su "casi di studio"*: al candidato viene proposta una situazione reale attinente alla specifica attività professionale. Egli dovrà fornire una risposta appropriata. Tale prova, integrata, se opportuna, da simulazioni (role-play), può consentire di valutare le abilità;
5) *simulazioni di situazioni reali operative (role-play)*: per valutare oltre alle abilità e alle competenze, anche le capacità personali (per esempio, capacità relazionali, comportamenti personali attesi);
6) *analisi e valutazione di lavori effettuati*: tale metodo comprende anche un confronto, in presenza del candidato, per approfondire la valutazione delle abilità, delle conoscenze e delle capacità relazionali;
7) *prove pratiche in situazioni operative attinenti alla realtà dell'attività professionale*: possono essere effettuate anche tramite osservazione diretta, durante l'attività lavorativa del candidato. Tale metodo può essere utilizzato per valutare le abilità e le competenze (comprese le capacità personali).

Va precisato che la scelta della combinazione dei metodi di valutazione deve considerare la tipologia dell'attività professionale e la necessità di rendere la valutazione delle conoscenze, abilità, autonomia e responsabilità, più completa e oggettiva possibile, per limitarne la discrezionalità.

2.8.6.5 Ulteriori certificazioni professionali

Di seguito si riportano ulteriori certificazioni, più riconosciute a livello mondiale, in merito alle competenze in cybersecurity:

- **Certified Information Security Manager** (CISM) di ISACA: è una certificazione delle competenze di sicurezza per gli IT Manager, in particolare delle competenze relative alle quattro aree di conoscenza alla base dell'Information Security Management, ossia: Information Security Governance, Information Risk Management & Compliance, Information Security Program Development & Management, Information Security Incident Management.

- **Certificazione Ethical Hacker** (CEH): attesta la capacità di portare, in modo etico, attacchi informatici a reti, infrastrutture IT, applicazioni e siti web sia dell'organizzazione per cui si lavora, sia a clienti, per individuare e risolvere vulnerabilità dei sistemi e migliorarne la sicurezza.

- **Certificazione CompTIA Network+**: convalida le competenze di base necessarie per realizzare, mantenere e risolvere i problemi (anche di sicurezza) delle reti aziendali.

- **Certificazione Cisco Certified Network Associate Security** (CCNA Security): comprova le conoscenze e le competenze per la messa in sicurezza delle reti Cisco, in particolare per sviluppare un'infrastruttura di sicurezza, riconoscere le minacce e le vulnerabilità delle reti Cisco e mitigare le minacce.

- **Certificazione CompTIA Security+**: dimostra le competenze necessarie per svolgere le funzioni di sicurezza di base.

- **Certificazione CompTIA Cybersecurity Analyst** (CySA+): attesta le conoscenze tecniche e le competenze necessarie per una figura di Security Analyst.

- **Certificazione CompTIA PenTest+**: convalida le competenze di un Penetration tester, ossia garantisce la capacità nell'ambito della pratica di "testare" un sistema informatico, una rete o un'applicazione web per trovare vulnerabilità di sicurezza che un utente malintenzionato potrebbe sfruttare, nonché di progettare e creare nuovi strumenti e test di penetrazione.

2.9 Il dominio Privacy - GDPR

Nel dominio della privacy e della tutela dei dati personali, il quadro normativo di riferimento è il Regolamento UE 2016/679 [2.15], noto come *General Data Protection Regulation* (GDPR; in italiano RGPD). In quanto Regolamento europeo, il provvedimento è vincolante in tutti i suoi elementi e direttamente applicabile in tutti gli Stati membri. È stato recepito dalla normativa italiana con il D.Lgs. 101/2018 [2.16], che ha recato modifiche al Codice in materia di protezione dei dati personali italiano (Codice della Privacy, D.Lgs. 196/2003) [2.17]. Il GDPR è composto da 99 articoli preceduti da 173 *considerando*, che offrono significativi approfondimenti interpretativi che costituiscono pertanto parte integrante e rilevante della norma. Il Regolamento si pone l'obiettivo di eliminare la frammentazione delle normative nazionali e garantire uniformità di disciplina a livello europeo. Risponde alle sfide poste dagli sviluppi tecnologici e dai nuovi modelli di crescita economica, tenendo conto delle esigenze di tutela dei dati personali dei cittadini dell'Unione europea. L'oggetto principale del GDPR è la protezione dei dati personali, visto come diritto fondamentale del cittadino. La norma sancisce anche il principio della libera circolazione dei dati all'interno dell'Unione europea, stabilendo che essa non può essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali. A tal fine, sorge la necessità di un Regolamento unico che garantisca certezza del diritto, trasparenza e coerenza del livello di protezione delle persone fisiche in tutta l'Unione. Nella vastità della norma, è utile tuttavia richiamare alcune definizioni, e successivamente, alcune prescrizioni fondamentali. Il GDPR definisce come "dato personale" qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato"); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale. Tuttavia, identifica dati personali specifici, attribuendo loro un maggiore grado di criticità:

- "dati genetici";
- "dati biometrici";
- "dati relativi alla salute".

All'art. 9, il GDPR individua però una speciale categoria di dati, chiamati dati personali particolari, come quei dati che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona. Per tali dati, con esclusione dei casi esplicitamente previsti dalla norma (esplicito consenso, obblighi in materia di diritto del lavoro, interesse vitale dell'interessato, trattamento necessario svolto all'interno di fondazioni o associazioni, finalità giudiziarie, ecc.) il trattamento è vietato.

I ruoli e le responsabilità principali identificate dal GDPR sono:

- **Titolare del trattamento**: 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; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri.

- **Responsabile del trattamento**: 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.

- **Destinatario**: rappresenta la persona fisica o giuridica, l'Autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le Autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette Autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento.

- **Data Protection Officer (DPO)**: obbligatorio per gli organismi o Autorità pubbliche, è designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti attribuitigli dalla norma. La nomina del DPO è adempimento obbligatorio anche quando il titolare effettua trattamenti che richiedono il monitoraggio regolare e sistematico degli interessati su larga scala oppure effettua come attività principali trattamenti su larga scala di dati sensibili, genetici, biometrici, giudiziari. I compiti del DPO sono quelli di informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal GDPR, vigilare affinché la norma sia applicata correttamente, fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliare lo svolgimento, cooperare con l'Autorità di controllo (in Italia il Garante per la Protezione dei Dati Personali) e fungere da punto di contatto per l'Autorità di controllo per questioni connesse al trattamento. Alcuni dettagli relativi alle procedure per il conseguimento del titolo di DPO sono illustrati nella sezione 3.3.

Il GDPR introduce alcuni principi basilari, su cui si fonda la liceità di un trattamento, principi che di fatto rappresentano la reale novità rispetto alla normativa preesistente nell'unione europea. I principali sono:

- **Principio dell'accountability**: il titolare deve essere in grado di dimostrare di avere adottato tutte le misure giuridiche, organizzative, tecniche, per la protezione dei dati personali, e deve dimostrare in modo proattivo che i trattamenti di dati effettuati sono adeguati e conformi al GDPR.

- **Principio della proporzionalità**: i dati devono essere adeguati e pertinenti alle finalità per le quali sono trattati, ed inoltre devono essere limitati a quanto necessario (minimizzazione).

- **Principio della privacy by design e privacy by default**: è necessario approcciare la tutela dei dati personali ponendo essa fin da subito come elemento rilevante nella progettazione delle

attività nelle organizzazioni, garantendo così gli strumenti e le corrette impostazioni. La privacy, oltre a essere incorporata nel progetto, deve essere adottata come impostazione di default.

Lo stesso art. 25, che introduce il principio della privacy by design (e by default), introduce l'elemento probabilmente più innovativo: il principio secondo il quale l'intero processo di adozione delle prescrizioni imposte dal GDPR in merito alla progettazione dei trattamenti deve avvenire secondo un approccio risk-based. La responsabilità del titolare e del responsabile del trattamento, si misura in termini di adeguati trattamenti del rischio di compromissione dei dati personali, tenendo conto della natura, della portata, del contesto e delle finalità del trattamento, nonché della probabilità e della gravità dei rischi per i diritti e le libertà degli utenti. Il GDPR adotta quindi il concetto di rischio informatico quale strumento fondamentale per guidare l'azione delle organizzazioni nella definizione dei trattamenti dei dati personali e misurarne la loro conformità alle prescrizioni imposte dalla norma. Rischio a cui si dà una precisa definizione nei considerando 75 e 76.
Un aspetto di cruciale importanza su cui il GDPR pone l'accento è la nozione di identificabilità dell'interessato. All'art. 4 comma 1, si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale. Il comma 5 dello stesso articolo introduce però il concetto di pseudonimizzazione, visto come trattamento applicato ai dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile. I considerando n. 26 e 75 chiariscono il significato della pseudonimizzazione, nonché la differenza con l'anonimizzazione, in relazioni agli obblighi in capo al titolare derivanti dal GDPR nel caso di trattamenti operati secondo le due tecniche. Circa il ruolo dell'anonimizzazione, lo stesso considerando sancisce che "il regolamento non si applica pertanto al trattamento di tali informazioni anonime, anche per finalità statistiche o di ricerca". Un altro elemento di rilevante importanza introdotto dal GDPR è l'obbligo di notifica di eventuali data breach a carico del titolare. All'art. 42, 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. 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 (GPDP) ha deciso di affidare ad Accredia l'accreditamento degli schemi di certificazione, che dovranno essere approvati dal Garante stesso.

2.10 Settore finanziario

Il settore finanziario è stato tra i primi ad abbracciare le opportunità offerte dalla digitalizzazione dei processi e delle operazioni. La crescita del mondo dell'informatica negli anni '70 e '80 del secolo scorso è almeno in parte dovuta alla forte spinta propulsiva fornita dalle applicazioni del calcolo automatico e delle telecomunicazioni proposte proprio dal settore finanziario. Forse, proprio per questo motivo, **il settore finanziario ha da sempre tenuto in debita considerazione i rischi legati alla cybersecurity.**

L'uso sempre più pervasivo di strumenti elettronici per lo scambio di moneta, anche attraverso reti pubbliche (Internet), insieme alla continua evoluzione dei profili di rischio associati ad attività criminali in ambito cyber, hanno imposto negli ultimi anni a livello internazionale una revisione delle regolamentazioni di settore. In questo contesto si sovrappongono diversi interventi provenienti principalmente a livello nazionale dalla Banca d'Italia e a livello europeo dall'Unione europea e dall'European Banking Authority (EBA).

2.10.1 Circolare n. 285 del 17 dicembre 2013

La circolare [2.18] è stata pubblicata dalla Banca d'Italia in data 17 dicembre 2013 e raccoglie le disposizioni di vigilanza prudenziale applicabili alle banche e ai gruppi bancari italiani. Il testo viene regolarmente aggiornato per adeguare la normativa interna alle novità che intervengono a livello internazionale in tema di regolamentazione. Alla data di scrittura di questo rapporto la circolare è al 38° aggiornamento pubblicato il 22 febbraio 2022. Il testo ha obiettivi molteplici, tra i quali quello di rendere possibile l'applicazione di una serie di misure volte a migliorare la gestione del rischio e la governance degli istituti bancari, sia a livello di sistema (riforme macroprudenziali) sia di singola organizzazione (riforme microprudenziali). La circolare è articolata in quattro parti, ciascuna suddivisa in più titoli, a loro volta caratterizzati da numerosi capitoli divisi in sezioni, per un totale di circa 780 pagine. Gli aspetti legati alla sicurezza delle informazioni e dei sistemi IT che vengono usati per gestire le stesse è trattata in modo particolare nel Titolo IV nei capitoli dedicati al Sistema Informativo (cap. 4) e alla Continuità Operativa (cap. 5).
Titolo IV, Capitolo 4: indica i requisiti che devono essere soddisfatti dalle organizzazioni in merito alla gestione del sistema informativo inclusivo delle risorse tecnologiche – hardware, software, dati, documenti elettronici, reti telematiche – e delle risorse umane dedicate alla loro amministrazione. I requisiti sono di carattere generale, mentre viene rimandata alle scelte strategiche proprie dell'organizzazione l'adozione delle best practice di riferimento per lo specifico settore. Riguardo ai temi della sicurezza dei sistemi informativi risultano particolarmente rilevanti le seguenti sezioni:

- Sezione II: definisce le funzioni organizzative delegate alla gestione dei sistemi informatici dettagliando i compiti dell'organo di supervisione strategica, dell'organo di gestione, l'articolazione organizzativa della funzione ICT, la funzione di sicurezza informatica, la gestione del rischio informatico e del rispetto delle norme e la funzione di *internal audit*;

- *Sezione III*: descrive il processo di analisi del rischio informatico;

- *Sezione IV*: descrive "i processi e le misure volti [...] a garantire a ciascuna risorsa informatica una protezione, in termini di riservatezza, integrità, disponibilità, verificabilità e *accountability*, appropriata e coerente lungo l'intero ciclo di vita". La sezione in particolare dettaglia le politiche di sicurezza, la sicurezza delle informazioni e delle risorse ICT, la gestione degli incidenti, la disponibilità delle informazioni e dei servizi;

- *Sezione V*: descrive il sistema di registrazione e reporting dei dati, strumento fondamentale per garantire l'accountability delle operazioni;

- *Sezione VI*: definisce i requisiti per l'esternalizzazione dei servizi ICT.

Titolo IV, Capitolo 5: è dedicato alla definizione dei requisiti legati alla continuità operativa dell'organizzazione. In particolare, la sezione II tratta la definizione del piano di continuità operativa e gestione delle crisi, anche in riferimento a incidenti cyber.

2.10.2 Payment Service Directive 2 (2015/2366/EU)

La Direttiva EU 2015/2366 [2.19] nota come Payment Service Directive 2 o PSD2, ha come obiettivo la promozione e lo sviluppo di un mercato interno dei pagamenti al dettaglio efficiente, sicuro e competitivo rafforzando la tutela degli utenti dei servizi di pagamento, sostenendo l'innovazione e aumentando il livello di sicurezza dei servizi di pagamento elettronici. La PSD2 disciplina i servizi di pagamento e, per quanto riguarda i servizi erogati attraverso reti e sistemi informatici, fornisce alcune indicazioni relative alla loro sicurezza. In particolare:

- Artt. 66-72 forniscono alcune indicazioni relative alle credenziali di accesso degli utenti, alla sicurezza dei canali di comunicazione utilizzati, e alle operazioni di autenticazione ed esecuzione delle operazioni di pagamento.
- Art. 94 definisce le modalità di protezione dei dati.
- Art. 95 discute la gestione dei rischi operativi e di sicurezza.
- Art. 96 definisce i requisiti legati alla notifica degli incidenti.
- Artt. 97 e 98 discutono i requisiti per i sistemi di autenticazione.

2.10.3 EBA Guidelines on ICT and security risk management (EBA/GL/2019/04)

Le EBA Guidelines on ICT and security risk management (EBA/GL/2019/04) [2.20] sono definite a partire dalle precedenti EBA Guidelines on the security measures for operational and security risks of payment services (EBA/GL/2017/17), che vengono di fatto sostituite, generalizzando la loro applicabilità dai soli sistemi di pagamento a tutti gli istituti che trattano il credito e gli investimenti. Il documento si focalizza sulla gestione del rischio dei sistemi ICT e della relativa sicurezza, riconoscendo il ruolo centrale che questi giocano nelle organizzazioni finanziarie. Forniscono dettagli su come gli istituti finanziari dovrebbero adeguarsi in merito alla gestione dei rischi ICT e di sicurezza, in accordo con l'art. 74 della Capital Requirements Directive (CRD) 2013/36/EU e l'art. 95 della PSD2. In particolare, le Linee Guida affrontano i seguenti punti:

- Sezione 3.2: focalizzata sulla gestione e mitigazione dei rischi ICT e di sicurezza attraverso l'adozione di una solida governance e di un framework di controllo interno che definisca chiare responsabilità per il personale, inclusi i membri del management.

- Sezione 3.3: impone l'adozione di una funzione di controllo interna, così come di un sistema indipendente di audit. Richiede che l'istituto finanziario mantenga una mappa aggiornata delle proprie business unit, dei processi a supporto e degli asset informativi, classificando la criticità sulla base della confidenzialità, integrità e disponibilità dei relativi dati.

- Sezione 3.4: definisce i requisiti per l'implementazione di misure efficaci di information security, incluse la definizione di opportune policy, la definizione di processi per la gestione e il testing delle misure di sicurezza, fino alla definizione di programmi di addestramento per il personale.

- Sezione 3.5: specifica una serie di principi di alto livello su come i sistemi ICT dovrebbero essere gestiti. Tra i vari aspetti toccati in questa sezione relativamente all'operatività dei sistemi ICT, viene anche raccomandata la definizione di opportuni processi di gestione degli incidenti.

- Sezione 3.7: affronta il problema della continuità operativa attraverso la definizione di piani di risposta e recupero a fronte di incidenti.

- Sezione 3.8: è dedicata alla sicurezza per i payment service providers (PSPs).

2.10.4 EBA Guidelines on outsourcing arrangements (EBA/GL/2019/02)

Le EBA Guidelines on outsourcing arrangements (EBA/GL/2019/02) [2.21] forniscono indicazioni per la corretta gestione dell'outsourcing. Negli ultimi anni, infatti, anche gli operatori finanziari hanno iniziato a fare un uso sempre più esteso di servizi offerti da terze parti (outsourcing). L'outsourcing di specifiche funzioni, pur aprendo il mercato a nuovi attori e incentivando la nascita di servizi innovativi, porta inevitabilmente a un incremento delle potenziali superfici di attacco e richiede quindi un'attenta valutazione dei relativi profili di rischio. Tra i tanti aspetti toccati da queste Linee Guida, risulta di particolare importanza per la presente trattazione la sezione 13.2. che definisce i requisiti di alto livello inerenti la sicurezza dei dati e dei sistemi, laddove questi siano oggetto di gestione da parte di un terzo. Altrettanto rilevante è quanto previsto al punto 91.b e successivi, ove si specifica che gli Enti e istituti di pagamento possono avvalersi di "certificazioni di soggetti terzi e relazioni di soggetti terzi o dell'audit interno messe a disposizione dal fornitore di servizi" per la valutazione dei fornitori di servizi esternalizzati.

2.10.5 Revised Guidelines on major incident reporting under PSD2 (EBA/GL/2021/03)

Le *Revised Guidelines on major incident reporting under PSD2* [2.22] sono delle Linee Guida frutto di una revisione di quelle originali pubblicate inizialmente nel 2017. In accordo con l'art. 96 della già citata PSD2, questo documento definisce le Linee Guida per la corretta implementazione dei processi di gestione degli incidenti, della loro classificazione e della relativa notifica verso le organizzazioni nazionali appositamente designate.

Le Linee Guida sono suddivise nelle seguenti sezioni principali:

- Classificazione degli incidenti: definisce una procedura per la definizione del livello di severità di un incidente, fornendo tutti i criteri qualitativi e quantitativi necessaria per una corretta classificazione.

- Processo di notifica: definisce il processo di produzione dei report previsti in caso di incidente grave.

- Delega e consolidamento delle notifiche: stabilisce gli elementi essenziali per poter delegare il processo di notifica a terze parti.

- Operational e security policy: richiede che nelle policy di sicurezza e gestione delle operazioni le fasi di incident reporting siano presenti.

- Assessment della rilevanza dell'incidente.
- Condivisione delle informazioni.
- Comunicazione con le Autorità competenti.

Le Linee Guida forniscono inoltre un template di documento di notifica sotto forma di allegato.

2.10.6 Cyber Resilience Oversight Expectations for financial market infrastructures

Il *Cyber Resilience Oversight Expectations for financial market infrastructures* [2.23], pubblicato dalla Banca Centrale Europea nel dicembre 2018, riprende e integra il precedente Guidance on cyber resilience for financial market infrastructures (FMI) pubblicato nel 2016 dal Committee on Payments and Market Infrastructures (CPMI) e dallo International Organization of Securities Commissions (IOSCO).

Il testo si pone tre obiettivi principali:

1. fornire gli istituti finanziari delle indicazioni operative per migliorare il proprio livello di preparazione rispetto ai rischi cyber;
2. definire delle esplicite aspettative in questo contesto per gli Enti di vigilanza;
3. fornire quindi una base di discussione comune tra istituti ed Enti di vigilanza.

Le aspettative sono suddivise su tre livelli di crescente maturità: *evolving, advancing e innovating*. Questa suddivisione permette di usare le expectation anche come benchmark per valutare il livello di resilienza ai rischi cyber di istituti caratterizzati anche da natura e dimensioni molto diverse. Il documento è strutturato attraverso cinque principali categorie di gestione del rischio e tre componenti generali:

- Governance;
- Identification;
- Protection;
- Detection;
- Response and Recovery;
- Testing;
- Situational Awareness;
- Learning and Evolving.

Di particolare interesse è il riferimento frequente fatto dal documento a schemi di certificazione. In particolare, nella aspettativa 6 si raccomanda alle FMI l'implementazione di un *Information Security Management System* (ISMS) basato su standard riconosciuti, tra cui vengono citati ISO/IEC 27001, ISO/IEC 20000-1 e ISO/IEC 27103. L'aspettativa 8, inoltre, raccomanda una ispezione e revisione periodica dell'ISMS, anche attraverso meccanismi di audit e certificazione. Anche in questo documento si fa riferimento, seppur in modo meno dettagliato, all'uso di certificazioni per la valutazione delle terze parti fornitrici di servizi.

2.10.7 Digital Operation Resilience Act (DORA)

Il Digital Operation Resilience Act (DORA) una proposta legislativa [2.24] su cui la Commissione Europea ha iniziato a lavorare dal 2019, mirata a razionalizzare l'insieme dei Regolamenti vigenti in ambito di resilienza degli operatori finanziari che operano attraverso strumenti digitali.
Il draft è stato pubblicamente rilasciato nel settembre 2020 ed è attualmente oggetto di revisione finale in attesa del suo rilascio previsto nel 2022.

La proposta prevede i seguenti punti:

- Requisiti applicabili agli istituti finanziari in relazione a:
  - ICT risk management;
  - notifica degli incidenti relativi ai sistemi ICT alle Autorità competenti;
  - testing della resilienza nell'ambito delle operazioni svolte in ambito digitale;
  - information e intelligence sharing;
  - gestione efficace del rischio ICT per le terze parti.
  - Requisiti per la contrattualizzazione con fornitori terzi di servizi ICT.
  - Framework di vigilanza verso i fornitori di servizi ICT terzi.
  - Regole per la cooperazione tra gli enti di sorveglianza.

La proposta è applicabile a una vasta famiglia di differenti istituti finanziari, ma vale la pena citare il fatto che per la prima volta sono esplicitamente citate le organizzazioni che gestiscono criptovalute. Nel provvedimento, l'art. 24 richiama in modo formalmente improprio, ma a nostro parere inequivocabile data la ratio del provvedimento, ovvero l'accreditamento per i tester che svolgono test di penetrazione.

- Per lo svolgimento dei test di penetrazione basati su minacce, le entità finanziarie si avvalgono unicamente di tester che:
  - possano vantare il più alto grado di idoneità e reputazione;
  - possiedano capacità tecniche e organizzative e dimostrino esperienza specifica nel campo delle informazioni sulle minacce, dei test di penetrazione o dei test red team;
  - siano certificati da un ente di accreditamento in uno Stato membro o rispettino codici formali di condotta o quadri etici;
  - nel caso di tester esterni, è necessario che gli stessi forniscano una garanzia indipendente o una relazione di audit concernente la solida gestione dei rischi derivanti dall'esecuzione di test di penetrazione basati su minacce, compresi un'adeguata protezione delle informazioni riservate dell'entità finanziaria e il risarcimento dei rischi commerciali dell'entità finanziaria;
  - nel caso di tester esterni, siano debitamente e pienamente coperti da un'assicurazione di responsabilità professionale, anche contro i rischi di colpa e negligenza.

- Le entità finanziarie garantiscono che gli accordi conclusi con i tester esterni prevedano una solida gestione dei risultati dei test di penetrazione basati su minacce e che qualsiasi trattamento di tali risultati, comprese la generazione, l'elaborazione, la conservazione, l'aggregazione, la segnalazione, la comunicazione o la distruzione, non comporti rischi per l'entità finanziaria.

3. Analisi dei servizi accreditati per la cybersecurity

In questo capitolo vengono descritte le procedure per la richiesta, l'ottenimento e il mantenimento delle certificazioni rilevanti nell'ambito della cybersecurity. Come evidenziato dal capitolo 2, il contesto normativo e regolatorio di riferimento ha subito una rapida accelerazione nell'ultimo decennio in corrispondenza dell'utilizzo di strumenti informatici e telematici in un numero maggiore di contesti operativi aziendali. Di conseguenza è emersa l'esigenza di avere a disposizione schemi di certificazione relativi al soddisfacimento di misure di sicurezza volte a ridurre il rischio e l'impatto di attacchi cyber. La rapida evoluzione delle tecnologie, e del loro utilizzo in contesti applicativi e operativi molto diversi in termini degli impatti che un attacco cyber può causare, ha due effetti principali: da un lato l'esigenza di un continuo processo di aggiornamento delle norme tecniche *(standard)* rivolti alla certificazione di processi aziendali; dall'altro, la creazione di schemi *(framework)* che definiscono specifici controlli di sicurezza in ambito cyber e la loro relazione con gli schemi di certificazione esistenti. I *framework di cybersecurity* forniscono indicazioni operative specifiche in un determinato ambito tecnologico e applicativo, finalizzate a soddisfare i requisiti definiti in modo più generale negli standard tecnici. Molti di questi non hanno infatti, come ambito di riferimento esclusivo, il mondo cyber stesso, ma l'intero sistema aziendale.

Questo ha il pregio di integrare l'ambito cyber all'interno dei processi aziendali e non di considerarlo come un ambito a sé stante, slegato dal resto. Allo stesso tempo rende necessaria la definizione di schemi che, attingendo al più vasto spettro degli *standard di certificazione* di processo e di prodotto, consentano di legare una specifica tipologia di rischio cyber a controlli tecnico-operativi specifici a loro volta derivanti da standard di settore. Un lavoro rilevante in questo senso è stato svolto dal National Institute of Standards and Technology (NIST) con la pubblicazione del Cybersecurity Framework e, in Italia, dal Cybersecurity National Lab del CINI attraverso la redazione e il continuo aggiornamento del Framework Nazionale (cfr. sezione 2.9.2).

Nella rassegna che segue verranno esaminati i principali standard e le relative certificazioni rilevanti per il mondo cyber. Si noterà come il principio guida e ispiratore degli standard, nonché filo conduttore, è legato alla gestione e alla sicurezza dei dati e delle informazioni per le quali gli elaboratori elettronici e le reti di comunicazione costituiscono oggi il principale mezzo. Come evidenziato nel capitolo precedente, soprattutto con riferimento alle recenti iniziative della Unione europea e alla ancora più recente pubblicazione della Strategia da parte dell'ACN, è in corso un'opera di definizione di standard specifici per l'ambito cyber orientati a specificare i requisiti relativi non solo alla sicurezza di dati e informazioni, ma, più in generale, alla garanzia della continuità del servizio, aspetto sempre più necessario data la crescente dipendenza della società moderna da calcolatori e dalle relative reti di comunicazione.

Una visione di insieme degli standard, dei framework e della normativa di settore rilevante per il mondo cyber è riportata in Figura 3.1 [3.1]. Come si può apprezzare dallo schema, a ciascun settore (Pubblica Amministrazione, Telecomunicazione, Servizi Finanziari e Bancari, Infrastrutture Critiche, ecc.) sono associate le norme ISO pertinenti per l'ambito cyber e a queste si affiancano schemi e regolamenti prodotti o da organizzazioni di settore (es. PCI SSC per quanto riguarda i servizi di pagamento elettronico [3.2]) o da associazioni trasversali rispetto ai settori applicativi, ma verticali rispetto alle tecnologie informatiche (es. OWASP per quanto riguarda la sicurezza delle applicazioni web [3.3] o SAE per la sicurezza dei veicoli [3.4]). Come sarà evidente anche nei capitoli successivi, fatta eccezione per le certificazioni di prodotto Common Criteria ISO/IEC 15048 (The Common Criteria for Information Technology Security Evaluation – cfr. sezione 2.9.3) le attività di certificazione hanno l'obiettivo di incidere sulle modalità operative e organizzative di un dato soggetto relativamente alla misurazione, gestione e mitigazione del rischio cyber.

Figura 3.1 - Standard e framework per i fornitori di servizi e le organizzazioni

Fonte [3.1]

3.1 Accreditamento - Regolamento CE 765/2008

Il processo di certificazione viene condotto da organismi pubblici o privati accreditati per svolgere l'attività di verifica della conformità di processi, sistemi, prodotti, servizi, persone, ai sensi delle norme e degli standard. Nelle sezioni che seguono viene descritta la procedura attraverso la quale un organismo ottiene l'accreditamento, ovvero è riconosciuto idoneo a effettuare in modo rigoroso e super partes le verifiche di processi e prodotti e, di conseguenza, a rilasciare la relativa certificazione. In altre parole, l'accreditamento è il processo attraverso il quale Accredia attesta la capacità di un soggetto di rilasciare una o più certificazioni.

3.1.1 Le fasi del processo di accreditamento

Domanda di accreditamento
La domanda deve essere compilata in funzione della specifica attività per cui l'organismo (o il laboratorio) richiede l'accreditamento e deve contenere le procedure applicate al processo, gli organigrammi, i manuali di gestione, ecc. La domanda, corredata della documentazione richiesta, viene esaminata dai funzionari tecnici del Dipartimento Accredia di competenza (Certificazione e Ispezione, Laboratori di prova, Laboratori di taratura) per valutarne l'accettabilità sulla base dei requisiti richiesti dai Regolamenti generali e dai regolamenti tecnici applicabili per l'accreditamento. A esito positivo, Accredia comunica l'accettazione della domanda di accreditamento, unitamente alla proposta del preventivo tecnico economico. Le tariffe applicate dall'Ente per le attività di valutazione condotte durante il processo di accreditamento sono pubbliche e consultabili nel Tariffario Accredia.

Esame della documentazione
L'analisi dei documenti presentati con la domanda di accreditamento viene condotta da un gruppo di verifica incaricato dal Direttore del Dipartimento di competenza. Lo scopo è valutare la conformità dell'attività dell'organismo o del laboratorio ai requisiti previsti dai documenti normativi, nonché ai requisiti contrattuali previsti da Accredia. Qualora dall'esame risultino necessarie integrazioni o adeguamenti, all'organismo o al laboratorio viene richiesto di fornire i documenti mancanti o completare le informazioni carenti. A esito positivo, Accredia avvia le verifiche ispettive in sede, presso l'organismo o il laboratorio che richiede l'accreditamento e, nei casi applicabili, programma le verifiche in accompagnamento presso le organizzazioni clienti degli organismi.

Verifiche ispettive in sede
Le verifiche in sede sono condotte da un gruppo di verifica ispettiva, composto da ispettori ed esperti qualificati da Accredia e selezionati all'interno di appositi elenchi. Lo scopo delle verifiche è accertare che le modalità operative del soggetto che richiede l'accreditamento, relativamente alle attività svolte, siano conformi alle prescrizioni dei Regolamenti generali, dei Regolamenti tecnici applicabili e di ogni altro documento normativo generale e settoriale, nonché ai Regolamenti e alle procedure stabiliti dal richiedente, così come formalizzati nella documentazione relativa al sistema di gestione (manuale, Regolamenti, procedure, istruzioni, liste di controllo, qualifiche del personale, ecc.). Ogni verifica si conclude con un rapporto di valutazione. Se emergono semplici osservazioni, l'iter di accreditamento procede. Nel caso in cui si evidenzino lievi criticità, si effettuano ulteriori visite di valutazione. In presenza di non conformità, il processo di accreditamento può essere sospeso. A esito positivo, il documento riassuntivo delle valutazioni effettuate viene sottoposto all'esame del Comitato competente a deliberare l'accreditamento dell'organismo o laboratorio.

Verifiche ispettive in accompagnamento
Per l'accreditamento degli organismi di certificazione, ispezione e verifica, alla verifica ispettiva in sede seguono le visite in accompagnamento presso le organizzazioni clienti. Con quest'ultima espressione si intendono: le aziende, pubbliche o private, intestatarie delle certificazioni di sistemi di gestione aziendale e delle certificazioni di prodotto (licenziatarie dei marchi di certificazione); le aziende che si avvalgono dei servizi di ispezione e di verifica delle dichiarazioni di emissioni, i professionisti certificati. Gli esiti delle verifiche in accompagnamento seguono la stessa procedura prevista per le verifiche in sede. A esito positivo, il documento riassuntivo delle valutazioni effettuate viene sottoposto all'esame del Comitato di accreditamento competente.

Delibera dell'accreditamento
Il Comitato competente per l'attività per cui l'organismo o il laboratorio richiede l'accreditamento valuta la pratica e delibera. La concessione dell'accreditamento viene formalizzata mediante apposita convenzione stipulata tra Accredia e il soggetto accreditato e l'emissione del certificato a marchio Accredia. L'accreditamento e il relativo certificato sono validi per 4 anni. Le delibere e l'iscrizione del nominativo dell'organismo o del laboratorio sono pubblicate nelle banche dati del sito web di Accredia.

Sorveglianza periodica
Nel corso dei 4 anni di validità dell'accreditamento, Accredia svolge un'attività periodica di sorveglianza sull'attività dell'organismo o del laboratorio accreditato ai fini di verificarne il mantenimento dei requisiti di competenza, indipendenza e imparzialità e la regolare conformità alle norme e agli altri documenti applicabili.

Estensione dell'accreditamento
Nel corso dei 4 anni di validità, l'organismo o il laboratorio può chiedere l'estensione dell'accreditamento a nuove attività e sedi operative. L'estensione non prolunga la validità dell'accreditamento e non comporta la sottoscrizione di una nuova convenzione, salvo il caso di aggiunta di sedi accreditate. Un organismo può estendere l'accreditamento a nuovi schemi di certificazione o nuovi settori, all'interno dello schema già coperto; un laboratorio di prova può ampliare la gamma delle prove accreditate; un laboratorio di taratura può coprire nuovi settori metrologici e materiali di riferimento, diversificare i campi di misura e/o ridurre le incertezze di misura.

Rinnovo dell'accreditamento
Prima della scadenza del ciclo quadriennale di accreditamento, può essere avviata la procedura di rinnovo, secondo le stesse modalità previste per il primo accreditamento.

3.1.2 Benefici derivanti dall'accreditamento

I benefici legati all'accreditamento sono molteplici. L'accreditamento è un'attestazione della competenza di un organismo o laboratorio a svolgere determinate attività di valutazione della conformità, rappresentando quindi uno strumento essenziale per la fiducia che il mercato ripone nei risultati delle valutazioni. L'accreditamento garantisce la sussistenza di profili di imparzialità, competenza e adeguatezza degli organismi di valutazione della conformità che operano nel mercato. Di conseguenza, contribuisce a migliorare le caratteristiche oggettive (qualità di prodotti e servizi) e soggettive (caratteristiche degli operatori economici) dei mercati, risolvendo un problema di

asimmetria informativa tra una domanda oggi più esigente che in passato e un'offerta, conseguentemente, più complessa, che porterebbe a equilibri subottimali nel mercato delle valutazioni di conformità. Il riconoscimento del valore intrinseco di una valutazione di conformità accreditata da parte del mercato è legato anche alla disponibilità a pagare per una valutazione di terza parte indipendente. Al contempo, gli interventi di politica pubblica beneficiano di uno strumento tecnico che dona certezza rispetto ai risultati attesi. Esempi in questo senso sono la soddisfazione dei requisiti richiesti nei bandi di gara predisposti dalle stazioni appaltanti pubbliche e private attraverso le valutazioni di conformità accreditata; o lo svolgimento di specifiche attività in settori cogenti e regolamentati gestiti dalla Pubblica Amministrazione attraverso l'accreditamento per autorizzazioni, abilitazioni e notifiche. È significativo anche il contributo alla semplificazione dei processi amministrativi. Le norme tecniche semplificano i processi di identificazione dei requisiti e la valutazione di conformità accreditata, basata sulle stesse norme, alleggerisce il carico amministrativo del controllo di conformità per le pubbliche amministrazioni. In ultimo, caratteristica predominante dell'accreditamento ai sensi del Regolamento CE 765/2008, è la sua validità internazionale. Attraverso gli Accordi europei di mutuo riconoscimento (MLA - Multilateral Agreements) firmati da Accredia con gli Enti associati a European co-operation for Accreditation (EA) le valutazioni di conformità accreditate diventano un'attestazione autorevole, di terza parte, accettata in tutti i Paesi membri. Inoltre le associazioni internazionali come International Accreditation Forum (IAF) e International Laboratory Accreditation Cooperation (ILAC) con le quali EA firma specifici accordi, allargano tale validità in altre aree economiche fuori dall'Europa.

3.2 Sistemi di gestione della sicurezza delle informazioni (ISMS)

La certificazione attualmente più matura nell'ambito della cybersecurity e obbligatoria in diversi contesti applicativi è quella secondo la norma tecnica UNI CEI EN ISO/IEC 27001, già descritta nella sezione 2.8.1. A questa norma sono collegate le norme della famiglia ISO/IEC 27XXX che definiscono requisiti aggiuntivi e più specifici rispetto alla ISO/IEC 27001. I paragrafi che seguono analizzano le diverse fasi del processo di valutazione con cui si ottiene la certificazione e le relative verifiche periodiche necessarie per il mantenimento della stessa.

3.2.1 Riferimenti normativi

- **UNI CEI EN ISO/IEC 17021-1** (norma di accreditamento)
  "Valutazione della conformità - Requisiti generali per gli organismi che eseguono audit e certificazioni di sistemi di gestione".

- **UNI CEI EN ISO/IEC 27006** (norma di accreditamento)
  "Valutazione della conformità - Requisiti generali per gli organismi che eseguono audit e certificazioni di sistemi di gestione per la sicurezza delle informazioni". In particolare, l'Annex A "Competenze e abilità per il personale che svolge gli audit e opera nel processo di certificazione".

- **UNI CEI EN ISO/IEC 27006 AMD1** (norma di accreditamento)
  "Valutazione della conformità - Requisiti generali per gli organismi che eseguono audit e certificazioni di sistemi di gestione per la sicurezza delle informazioni" documento che introduce alcune modifiche alla Norma ISO/IEC 27006.

- **IAF Mandatory Document 13**
  "Requisiti di conoscenza per il personale che opera negli Enti di accreditamento sugli schemi riferiti ai sistemi di gestione per la sicurezza delle informazioni".

- **UNI CEI EN ISO/IEC 27001**
  "Requisiti per i sistemi di gestione per la sicurezza delle informazioni".

- **NORME DELLA FAMIGLIA ISO/IEC 27XXX**
  Definiscono requisiti aggiuntivi rispetto alla norma UNI CEI EN ISO/IEC 27001. È il caso della ISO/IEC 27017 "Prassi sui controlli per la sicurezza delle informazioni per i servizi in infrastrutture cloud" o della ISO/IEC 27018 "Requisiti per la protezione dei Dati Personali in infrastrutture cloud che operano come titolari o responsabili del trattamento di tali informazioni".

3.2.2 Il processo di certificazione

La domanda

Le organizzazioni che adottano la norma **UNI CEI EN ISO/IEC 2700**1 (nella versione in vigore al momento della decisione) devono necessariamente raggiungere un livello accettabile di adeguatezza del proprio sistema di gestione per la sicurezza delle informazioni, l'Information Security Management System (ISMS). Ciò avviene quando il sistema di gestione è adatto alle dimensioni e operatività dell'organizzazione, quindi a mitigare al livello desiderato gli specifici rischi che impattano sui processi e sul business. Nella valutazione è inclusa l'aderenza a tutti i requisiti normativi e la ragionevole adozione dei controlli operativi previsti a margine della valutazione dei rischi e della Business Impact Analysis (BIA). Stante questa condizione di operatività e di aderenza ai requisiti definiti dalla norma, dopo aver svolto almeno un ciclo di Audit Interni sul sistema di gestione e un Riesame della Direzione, l'organizzazione è pronta a richiedere l'intervento di un organismo di certificazione accreditato.

Far certificare il proprio sistema di gestione da un organismo che operi sotto accreditamento garantisce due vantaggi: il primo è quello di ricevere, con cadenza almeno annuale, una valutazione condotta da un team di auditor di provata esperienza, che consente di analizzare la reale operatività e adeguatezza del sistema di gestione e il suo livello di conformità ai requisiti normativi. Il secondo aspetto è proprio la comunicazione, rivolta al mercato, dell'esistenza, efficacia e conformità alla norma UNI CEI EN ISO/IEC 27001 (universalmente riconosciuta come standard di riferimento). Si tratta di una garanzia per tutte le parti interessate, che offre una ragionevole fiducia sulla capacità del sistema di gestione di garantire l'efficacia attesa e di dimostrare la propria conformità ai requisiti normativi.

La scelta dell'organismo di certificazione accreditato è normalmente basata su considerazioni di carattere commerciale e operativo. L'adeguatezza dell'offerta in termini di operatività, competenza e costi, normalmente rappresenta il criterio di scelta. Ad esempio, oltre alla tariffa applicata per le giornate di attività che si renderanno necessarie, si tiene conto del settore di attività economica di appartenenza (sanitario, bancario, industriale, produzione di energia elettrica, servizi IT, ecc.). Di fatto ognuno con proprie obbligazioni contrattuali e di legge che rappresentano dei vincoli intorno ai quali debbono essere strutturate le soluzioni per la continuità operativa e per il livello di servizio da garantire tramite l'infrastruttura IT ricompresa nel perimetro di applicazione del sistema di gestione.

Relativamente alla definizione del tempo di audit, **la norma ISO/IEC 27006** arricchisce di requisiti specifici per lo schema ISMS la norma generale di accreditamento UNI CEI EN ISO/IEC 17021-1 e introduce delle considerazioni di merito per il processo di certificazione. Per la valutazione del tempo di audit, si parte da un numero di giornate di riferimento, che è quello definito dal numero di persone che, per dirla con la norma, operano "sotto il controllo della stessa organizzazione". Si tratta di coloro che, seppure in misura diversa, hanno la possibilità di interagire con l'infrastruttura IT. Esistono anche altri criteri, a seconda che si tratti di persone che operano in modo continuativo o con modalità part-time o, comunque, discontinue. Inoltre, debbono essere presi in considerazione altri requisiti, quali, a titolo di esempio:

- Esigenza di tempo di audit addizionale per logistica complessa; per differenze linguistiche e conseguente esigenza di interpreti; per presenza di siti temporanei o remoti; per l'adozione di normative e requisiti aggiuntivi; per la presenza di un'infrastruttura IT complessa o con molte connessioni; per la concomitante criticità dei processi e complessità tecnologica dell'infrastruttura IT o di Disaster Recovery; per l'esistenza di processi critici dati in outsourcing.

- Possibilità di riduzione del tempo di audit per il basso rischio che impatta sui processi (infrastruttura IT elementare); per bassa complessità operativa, come nel caso di aziende che erogano un solo servizio; per il fatto che nell'organizzazione ci sono molte persone che svolgono la stessa mansione o con bassissimo impatto sull'infrastruttura IT; per la precedente conoscenza dell'organizzazione, già certificata per altri schemi o per la maturità del sistema.

La norma ISO/IEC 27006 indirizza anche le competenze specifiche del Team di Audit, prevedendo che gli auditor abbiano conoscenza e comprensione dei seguenti argomenti, ancorché a diversi livelli: programmazione e pianificazione degli audit; tipo e metodologie di audit; rischio di audit; analisi dei processi di sicurezza delle informazioni; miglioramento continuo; controllo interno della sicurezza delle informazioni. Oltre che su specifici aspetti legati alla regolamentazione: proprietà intellettuale; contenuto, protezione e conservazione dei record organizzativi; protezione dei dati e privacy; regolazione dei controlli crittografici; commercio elettronico; firme elettroniche e digitali; sorveglianza sul posto di lavoro; intercettazione delle telecomunicazioni e monitoraggio di dati (es. posta elettronica); abuso del computer; raccolta elettronica di prove; test di penetrazione; requisiti settoriali internazionali e nazionali (es. bancario).

Le fasi del processo di valutazione

Accettata l'offerta dell'organismo di certificazione, vengono definite le date per lo svolgimento del processo di audit iniziale, che comprende due fasi di valutazione dell'organizzazione.

La prima fase prevede che venga svolta un'analisi del "progetto" dello ISMS. Questo si svolge attraverso l'analisi della documentazione di sistema e delle registrazioni previste. Oltre a una visita al sito (o ai siti più pertinenti, se più di uno) dell'organizzazione, gli auditor incaricati realizzano interviste preliminari con la Direzione e le figure chiave nello sviluppo e nella gestione del ISMS, verificando se il sistema è attivo da un tempo sufficiente ad aver attivato il ciclo di Deming (almeno una iterazione sistemica) comprensivo degli Audit Interni e del Riesame della Direzione.

Dalla valutazione delle informazioni deriva la decisione di proseguire con l'iter di auditing. All'organizzazione viene dato un tempo congruo per correggere eventuali criticità rilevate, indicando quali di queste siano da considerare maggiormente critiche e tali da impedire la certificazione, ove non sanate. Nella seconda fase dell'audit iniziale viene svolta una valutazione operativa sul funzionamento dei controlli operativi e sulla effettiva applicazione di quei processi sistemici che costituiscono il sistema di gestione per la sicurezza delle informazioni. Sono analizzate le configurazioni dei dispositivi che compongono l'infrastruttura IT. A seconda delle complessità e dimensioni di tale infrastruttura e della dimensione e complessità dell'organizzazione, viene adottato un criterio di campionamento dei vari elementi sistemici, in modo da ricostruire con sufficiente fedeltà un quadro della reale applicazione e del funzionamento dell'ISMS. Vengono quindi intervistati i responsabili dei processi e gli stessi operatori che operano nel perimetro del sistema di gestione. Alcuni dei controlli operativi sono sottoposti a test, come nel caso degli apprestamenti per la continuità operativa e il ripristino da eventi catastrofici (Business Continuity e Disaster Recovery), al fine di verificare come i tempi di Recovery Time Objective e di Recovery Point Objective siano effettivamente conseguiti. Vengono verificate, ad esempio, le impostazioni e i sistemi di monitoraggio e difesa dei dispositivi portatili Mobile Device Management (MDM), il sistema di autorizzazione alla connessione all'infrastruttura IT, ad esempio con verifiche sull'Active Directory, la gestione dei Log di sistema e la gestione delle disposizioni regolamentari al proposito, le configurazioni dei firewall e dei bridge, degli switch programmabili o dei router. Sono altresì verificate le scelte dell'organizzazione in merito alla gestione delle possibili vulnerabilità e delle modalità di "patching" delle stesse. Ove presenti, si valutano le modalità adottate per lo sviluppo di software e le modalità di validazione (certificazione in gergo tecnico) dello stesso software e il passaggio dall'ambiente di sviluppo a quello di produzione, con le relative cautele, ma anche le modalità per la gestione dei Database e per la loro salvaguardia.
Al termine, il team di audit predisporrà un rapporto, nel quale si evidenziano gli aspetti dell'organizzazione considerati non conformi ai requisiti normativi, alle obbligazioni aziendali pertinenti, ma anche possibili debolezze nella valutazione dei rischi, nella BIA e nella conseguente struttura dei controlli operativi, con il "congelamento" della cosiddetta Statement of Applicability (SoA), un elenco dei controlli operativi adottati dall'organizzazione, principalmente di quelli esclusi e delle ragioni sottostanti. In assenza di non conformità maggiori, quindi di violazioni gravi dei requisiti della norma tecnica di riferimento UNI CEI EN ISO/IEC 17021-1 e/o di norme cogenti, oppure di situazioni tali da compromettere l'efficacia e la conformità dei processi del ISMS e/o dei controlli operativi, viene proposta la certificazione dell'organizzazione. Questa proposta, sottoposta al vaglio di funzionari tecnici competenti dell'organismo di certificazione, per completezza e correttezza delle registrazioni, assieme alla valutazione di altri aspetti amministrativi, viene infine valutata operativamente da specifiche risorse interne all'organismo con delega e competenza per assumere la decisione di rilasciare la certificazione. Superate tutte le fasi del processo di valutazione, viene emesso il certificato di conformità che riporta il nome e l'indirizzo dell'organizzazione licenziataria, la norma di riferimento (UNI CEI EN ISO/IEC 27001), il campo di applicazione e le date di validità dello stesso certificato.

La sorveglianza

Da questo momento, l'organizzazione licenziataria della certificazione deve sostenere degli audit di sorveglianza, di massima annuali. Alcune organizzazioni preferiscono scegliere una frequenza più elevata di audit, in modo da avere una maggiore garanzia del livello di servizio ricevuto sostenendone, evidentemente, i costi. In questo processo di valutazione continuo, gli organismi di certificazione sono chiamati a verificare che le organizzazioni mantengano attivo il proprio ISMS, che

deve essere efficace nel perseguire gli obiettivi di volta in volta definiti. Nella fattispecie, si tratta di obiettivi di protezione delle informazioni e dell'infrastruttura deputata a elaborarle, trasmetterle e/o memorizzarle. Gli auditor degli organismi, nell'ambito del processo di sorveglianza dei sistemi di gestione, possono anche esprimere dei pareri in merito a possibili migliorie, ma si astengono dal dare indicazioni sul "come" raggiungere i risultati in ottica di conformità o di migliore efficacia e/o efficienza, essendo questa una specifica responsabilità dell'organizzazione. Uno dei principi alla base delle attività di un organismo di certificazione è, infatti, l'indipendenza e l'assenza di conflitti di interessi, oltre alla garanzia di riservatezza.
Alcuni dei principi alla base della certificazione sono: la trasparenza sulle procedure e Regolamenti che hanno portato al suo rilascio; la gestione dei reclami e segnalazioni su possibili comportamenti scorretti delle organizzazioni licenziatarie delle certificazioni; la responsabilità sulla conformità e adeguatezza dello ISMS in capo all'organizzazione (mentre l'organismo di certificazione è responsabile della competenza, prudenza e perizia, nonché del rispetto delle regole applicabili nel processo di certificazione, nel suo complesso). Un impatto rilevante sulla credibilità e utilità del processo di certificazione deriva dal costante mantenimento delle competenze delle risorse umane incaricate di gestire, nelle diverse fasi, il processo di valutazione e certificazione.
In tutto il processo di certificazione, e ancora di più in quello di sorveglianza, l'organismo di certificazione deve programmare i propri interventi di audit con un approccio basato sulla valutazione dei rischi. Per questo, i funzionari degli organismi devono confrontarsi con i Lead auditor, per valutare quali priorità dare agli elementi da valutare. Ne discendono le considerazioni e il criterio di campionamento utilizzato nel processo di pianificazione ed esecuzione degli audit. Nel pianificare gli audit di sorveglianza, infine, si deve tener conto della garanzia da offrire in termini di imparzialità reale e percepita, selezionando auditor che non abbiano maturato, ad esempio, una eccessiva confidenza con l'organizzazione. In questo risiede il mantenimento di un delicato equilibrio. Andare più volte a valutare la conformità dello ISMS di una stessa organizzazione può garantire una migliore conoscenza dei processi e dei controlli operativi adottati, ma, al contempo, può comportare il rischio di un'eccessiva familiarità con le risorse umane aziendali e un'aspettativa di conoscenza dei processi e dei rischi correlati dell'organizzazione, che nel frattempo sono destinati a cambiare.

Il rinnovo

Dopo 3 anni dalla data di delibera della certificazione, l'organizzazione può scegliere di rinnovare il contratto di certificazione con l'organismo. Questo processo avviene con qualche mese di anticipo rispetto al triennio, per evitare il rischio che scada la validità del certificato di conformità. La fase di rinnovo richiede un'analisi accurata delle eventuali modifiche avvenute nell'organizzazione, nonostante le valutazioni già fatte in occasione delle sorveglianze. Viene condotta un'attenta valutazione del percorso fatto dall'organizzazione nei 3 anni di certificazione. E' un momento importante di analisi dei rapporti di audit e delle relative registrazioni pertinenti ai 3 anni di validità della certificazione, delle evidenze di audit raccolte, delle risultanze e in particolare dei rilievi, ma soprattutto della maturità dimostrata nella loro gestione. Sulla base di queste informazioni viene "affinato" il calcolo del tempo di audit necessario per il rinnovo, che, in condizioni normali, è di circa due terzi del tempo che è stato necessario, a suo tempo, per la verifica iniziale del sistema di gestione. L'organizzazione, basandosi anche su considerazioni di prezzo, può decidere di cambiare organismo di certificazione. Il processo di accreditamento garantisce che tutti gli organismi di certificazione siano allineati sul rispetto dei requisiti minimi di accreditamento, intesi come rispetto dei principi indicati dalla norma UNI CEI EN ISO/IEC 17021-1.

Tuttavia, ogni organismo di certificazione deve sforzarsi di differenziare la propria offerta. Ciò può avvenire sia con una riduzione delle tariffe, sia attraverso specializzazioni ed eccellenze, come la capacità di operare in specifiche aree tecniche (industrie manifatturiere con infrastrutture "OT" o regolamentate come quelle finanziarie, ovvero sanitarie, ove i rischi sono di altissimo potenziale per la vita dei pazienti, ecc.).

Le attese nei confronti degli ISMS nelle organizzazioni

Lo sviluppo di un sistema di gestione per la sicurezza delle informazioni o, meglio, integrato tra sicurezza delle informazioni e cybersecurity, riduce in modo significativo il livello di rischio nell'esposizione alle minacce. Una riduzione che è tanto più significativa quanto più il sistema di gestione viene sviluppato, processo per processo, a partire dalla valutazione del contesto interno ed esterno, dalla valutazione dei rischi e dalla BIA, con attenzione, con diligenza, con capacità di immaginare gli scenari e le minacce possibili e mantenendo sempre aggiornati i sistemi a fronte delle possibili vulnerabilità. Una delle vulnerabilità più critiche è quella rappresentata dai comportamenti non prudenti delle risorse umane che possono interagire con le infrastrutture da proteggere. La diligenza nella gestione di un'infrastruttura IT è dunque direttamente proporzionale all'impegno nella formazione e addestramento, nonché alla creazione di consapevolezza delle risorse umane.

3.3 Ispezioni e verifiche sulla sicurezza delle informazioni e cybersecurity

Nel seguito si presentano gli aspetti relativi alle ispezioni e alle verifiche della sicurezza delle informazioni che sono necessarie al fine di stabilire il grado di sicurezza del sistema di gestione e trattamento delle informazioni aziendali. L'organismo che effettua ispezione e verifiche deve sottoporsi alla procedura di accreditamento al pari di un organismo di certificazione, come richiamato nella sezione 3.1. Accredia verifica dunque che l'organismo di ispezione soddisfi i requisiti della norma tecnica di accreditamento UNI CEI EN ISO/IEC 17020, in termini di competenza, imparzialità e riservatezza del personale coinvolto nelle attività ispettive; che le procedure di ispezione siano conformi alle norme applicabili e come gli ispettori dell'organismo effettuano le proprie attività di ispezione coerentemente con le procedure redatte dall'organismo. Allo scopo non è sufficiente solo una verifica documentale sul sistema di gestione dell'organismo, ma occorre effettuare anche delle verifiche in accompagnamento in cui gli ispettori di Accredia osservano il comportamento dell'ispettore dell'organismo presso le varie organizzazioni. In considerazione dell'oggetto di ispezione, Accredia si avvale di alcuni esperti tecnici dell'ambito cybersecurity sia durante le verifiche in sede che durante le verifiche in accompagnamento.

3.3.1 Riferimenti normativi

- **UNI EN ISO/IEC 17020**
  "Valutazione della conformità: Requisiti per il funzionamento di vari tipi di organismi che effettuano attività di ispezione".

- **Framework Nazionale per la Cybersecurity e la Data Protection** versione 2.0 di febbraio 2019.

3.3.2 Contesto di riferimento

Il *Framework Nazionale per la Cybersecurity* e la *Data Protection* si pone l'obiettivo di supportare le aziende nella individuazione delle vulnerabilità del loro sistema di trattamento delle informazioni e procedere, se è il caso, a rafforzarlo minimizzando il rischio di incidenti e di danni ingenti. Come illustrato nella sezione 2.8.2, il Framework si sviluppa, in maniera gerarchica, in *function, category e subcategory*. Tali elementi sono generali e sono indipendenti rispetto al settore produttivo, alla tipologia degli impiegati, alla dimensione e alla dislocazione sul territorio dell'organizzazione.

3.3.3 Il processo di ispezione

Sulla base di questo Framework sono state sviluppate determinate check list che sviluppano e attualizzano, a seconda del tipo di organizzazione che richiede il servizio, le function del Framework. Tali check list vengono sottoposte alle organizzazioni per valutare le previste attività abilitanti, con il fine di misurare la capacità di garantire la sicurezza delle informazioni trattate e l'assenza di potenziali esposizioni ad attacchi cyber del proprio sistema di sicurezza. Il compito dell'ispettore e dell'esperto Accredia è proprio quello di entrare nel merito dell'attività ispettiva valutandone la conformità alle function del Framework, oltre che all'abilità e alla competenza dell'ispettore nel valutare i risultati ottenuti.

Validità del rapporto di ispezione rilasciato
La validità del rapporto di ispezione rilasciato è relativa al momento in cui si effettua la verifica. Il risultato cioè non ha validità nel tempo, ma evidenzia lo stato del sistema di sicurezza per la gestione delle informazioni al momento in cui si effettua la verifica. È, in altre parole, lo "stato di salute" in cui versa il sistema di sicurezza delle informazioni aziendale al momento dell'ispezione.

Conseguenze dell'esito del rapporto di ispezione
Una volta noto lo stato del sistema di sicurezza, l'organizzazione può decidere se:

- attuare o meno altre misure di controllo più approfondite sugli aspetti del sistema per la sicurezza delle informazioni che hanno ottenuto un punteggio basso (per esempio effettuando vulnerability assessment o penetration test);
- adottare misure per aumentare la solidità del sistema per la sicurezza delle informazioni gestite;
- accettare il punteggio basso ottenuto accollandosi il rischio di essere un soggetto più vulnerabile agli attacchi informatici e correre il rischio di perdita della confidenzialità, integrità o disponibilità delle informazioni.

Queste conseguenze esulano dal mandato dell'attività ispettiva, in quanto rientrano in attività di consulenza, attività non ammissibile per un organismo di ispezione.

3.4 Vulnerability Assessment

Una componente importante nella attività di certificazione relativa alla cybersecurity è la verifica della presenza di vulnerabilità note, cioè di elementi di debolezza del sistema che possono consentire a un soggetto malintenzionato di ottenere informazioni, di alterare le informazioni presenti nel sistema, di alterare il funzionamento del sistema preposto alla gestione delle informazioni o, infine, di bloccare in tutto o in parte le funzionalità di un sistema.
Queste attività di verifica seguono specifiche procedure e richiedono che il laboratorio di prova accreditato che le esegue soddisfi requisiti in materia di competenza, imparzialità, riservatezza (come illustrato nella sezione 3.1 e nella sezione 3.3).

3.4.1 Riferimenti normativi

- **UNI CEI EN ISO/IEC 17025** (norma di accreditamento)
  "Requisiti generali per la competenza dei laboratori di prova e taratura".

- **NIST SP 800-115**
  "Technical Guide to Information Security Testing and Assessment".

- **NIST SP 800-37**
  "Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy".

- **NIST SP 800-53**
  "Security and Privacy Controls for Information Systems and Organizations".

3.4.2 Contesto di riferimento

Per illustrare il processo di Vulnerability Assessment (VA) si consideri lo scenario attuale caratterizzato da una crescente digitalizzazione della vita economica e amministrativa del Paese. Ad esempio, l'accesso ai numerosi servizi offerti dalla Pubblica Amministrazione richiede la disponibilità di servizi digitali che assicurino la certa identificazione di persone fisiche e giuridiche soprattutto per i servizi aventi valore legale ed elevatissimo valore commerciale. Gli operatori che erogano i servizi connessi all'identità e all'identificazione trattano informazioni altamente critiche dal punto di vista della riservatezza e devono garantire elevatissimi livelli di disponibilità dei propri servizi.

Tra questi figurano:

- i servizi fiduciari (firma digitale, certificati SSL, marche temporali, ecc.) erogati in applicazione del Regolamento UE 910/2014 (eIDAS);
- il Sistema Pubblico per la gestione dell'Identità Digitale (SPID);
- i servizi di conservazione a norma dei documenti informatici, disciplinati dal Codice dell'Amministrazione Digitale (CAD) e normative collegate.

Il percorso autorizzativo degli operatori che erogano tali servizi, governato in Italia dall'AgID, prevede che essi vengano sottoposti a valutazione da parte di organismi di certificazione accreditati (a norma UNI CEI EN ISO/IEC 17021-1) e laboratori di prova accreditati (a norma UNI CEI EN ISO/IEC 17025) circa l'idoneità tecnica dei servizi erogati e delle misure di sicurezza da essi adottate. In particolare, è previsto che i sistemi informatici utilizzati da questi operatori vengano periodicamente sottoposti a Vulnerability Assessment (VA) e Penetration Testing (PT) da parte di laboratori di prova accreditati.
Infatti, la norma UNI CEI EN ISO/IEC 27001 che descrive le migliori pratiche per un ISMS (cfr. sezione 3.2) richiama nell'Allegato A la necessità di adottare un processo di gestione delle vulnerabilità e, in particolare, il controllo A.12.6.1 definisce come l'organizzazione debba adottare criteri per impedire lo sfruttamento di eventuali vulnerabilità tecniche e gestire i relativi rischi.
Al fine di cogliere l'obiettivo descritto dal controllo, le vulnerabilità devono essere conosciute dall'organizzazione, pertanto l'analisi delle vulnerabilità sui sistemi informatici diviene lo strumento indispensabile per una coerente gestione del rischio.

3.4.3 L'esecuzione del Vulnerability Assessment

Qualsiasi sistema informatico può presentare falle di sicurezza (le cosiddette vulnerabilità) che possono consentire a terzi (hacker malevoli, dipendenti infedeli, ecc.) di provocare danni, degrado o interruzione dei servizi o anche l'accesso ai sistemi, con distruzione oppure furto di informazioni e/o di identità. Le categorie di vulnerabilità dei sistemi informatici sono periodicamente aggiornate e rese disponibili attraverso il servizio Common Weakness Evaluation (CWE)[23], mentre CVE[24] e NVD[25] elencano le vulnerabilità individuate in specifiche versioni di software e hardware e le relative misure per la loro risoluzione. Durante i test, il laboratorio accreditato esegue un'analisi approfondita dei sistemi dell'operatore, per verificare se esistono vulnerabilità note. I test possono essere eseguiti sia sulla componente network che sulle componenti applicative, ossia i software che erogano i servizi. Se vengono riscontrate vulnerabilità, il laboratorio può eseguire, previo accordo con l'operatore, anche il Penetration Testing (PT) ossia tentativi di sfruttare le vulnerabilità per verificare, nella configurazione complessiva dei sistemi e delle attività eseguite dall'operatore, la tipologia di danni o di accessi che tali vulnerabilità possono consentire a un soggetto attaccante. Con il PT è possibile individuare vulnerabilità non note a priori. Il processo di individuazione delle vulnerabilità, se posto sotto accreditamento, necessita di un approccio metodologico formalmente definito, che definisca in modo adeguato le modalità con le quali sono selezionati gli strumenti automatici di analisi, le modalità di selezione e verifica delle competenze del personale che esegue le attività di VA e, infine, delle modalità di documentazione delle minacce e dei rischi individuati (rapporto di prova). Queste modalità devono soddisfare i requisiti formali e sostanziali stabiliti dalla **norma di accreditamento UNI CEI EN ISO/IEC 1702**5. Un laboratorio di prova che desidera essere accreditato per le prove di VA deve innanzitutto predisporre la documentazione che descrive gli aspetti organizzativi ed operativi delle attività di VA. Questa documentazione verrà poi inviata ad Accredia insieme con la domanda di accreditamento. La procedura di accreditamento dei laboratori di prova si svolge come descritto nel Regolamento Generale Accredia RG-02, integrato, per quanto riguarda i laboratori che eseguono attività di VA, dalla Circolare n. 1/2019/DL del 28 dicembre 2019 che fornisce indicazioni aggiuntive e specifiche.

---

[23] *https://cwe.mitre.org*
[24] *https://cve.mitre.org*
[25] *https://nvd.nist.gov*

La documentazione predisposta dal laboratorio viene valutata da Accredia per verificarne la conformità con i requisiti previsti dalla norma di accreditamento e con quelli stabiliti nei metodi di prova (nel caso dei laboratori accreditati per VA, i documenti della serie NIST SP 800 menzionati al par. 3.4.1). Qualora questi documenti presentino difformità rispetto ai requisiti richiesti, oppure siano lacunosi nella descrizione delle modalità organizzative ed operative, Accredia ne chiede la revisione. Questa fase del processo di accreditamento, che richiede al laboratorio di prova di fornire una descrizione approfondita delle proprie modalità organizzative e operative, permette anche al laboratorio di auto esaminarsi, di confrontarsi con i requisiti di accreditamento e di allinearsi a essi. Ottenuti i documenti conformi, Accredia esegue un audit presso il laboratorio, allo scopo di verificare se quanto descritto nei documenti è effettivamente messo in pratica e se il personale e le dotazioni strumentali sono idonee a eseguire correttamente i metodi di prova. L'audit è eseguito da un gruppo di valutazione composto da un ispettore incaricato del coordinamento (team leader) che valuta la conformità degli aspetti organizzativi ed il rispetto dei requisiti generali di accreditamento stabiliti nella norma UNI CEI EN ISO/IEC 17025, validi per laboratori di prova operanti in qualsiasi settore tecnologico, e da uno o più ispettori ed esperti tecnici con competenze specifiche in VA e cybersecurity.

Un **Vulnerability Assessment (VA)** si svolge in 5 fasi:

1. Preparazione
Viene stabilito il perimetro oggetto di test e sono individuati tutti gli asset (dispositivi e sistemi) che saranno oggetto di analisi da parte del laboratorio accreditato:

- rete e suoi componenti, sia di tipo cablato che wireless;
- server, workstation, personal computer e altri dispositivi connessi alla rete quali tablet, stampanti, telecamere, ecc.;
- database o repository che contengono grandi quantità di dati;
- applicazioni, di tipo client/server, web-based, o implementate su dispositivi mobili quali cellulari, tablet, ecc.

Vengono inoltre stabiliti tempi e modalità di esecuzione dei test, eventuali attività che debbono essere effettuate dal cliente per favorire l'esecuzione dei test, e vengono stabilite le rispettive responsabilità, generalmente con un patto di manleva.

2. Esecuzione dei test
Il laboratorio di prova esegue la verifica della presenza o meno di vulnerabilità note scansionando i sistemi dell'operatore con strumenti automatici. In relazione al profilo di rischio e, di conseguenza, al profilo di certificazione richiesta, possono essere eseguite analisi più approfondite attraverso strumenti semi-automatici o sviluppati ad hoc, finalizzati a individuare ulteriori vulnerabilità note o debolezze specifiche non individuabili immediatamente attraverso strumenti di analisi automatica. La scansione può essere effettuata dall'interno della rete dell'operatore, oppure dall'esterno, a seconda del tipo di sistemi che devono essere valutati, della profondità dell'analisi che si desidera effettuare, e delle indicazioni tratte da eventuali precedenti incidenti di sicurezza, che in qualche caso potrebbero aver avuto origine dall'interno dell'organizzazione valutata.

3. Analisi dei risultati
Una volta individuate ed elencate tutte le vulnerabilità presenti nei sistemi oggetto di test, il laboratorio di prova le esamina singolarmente, elimina gli eventuali "falsi positivi" risultanti dalle scansioni automatizzate, e le associa alle informazioni di dettaglio eventualmente disponibili nei database internazionali che ne indicano l'origine e l'importanza.

4. Valutazione dei rischi
Le vulnerabilità vengono esaminate dal punto di vista della loro pericolosità considerata relativamente alla configurazione dei sistemi dell'operatore e, ove possibile, ai modi d'uso degli stessi. Una medesima vulnerabilità, rilevata in contesti diversi può infatti presentare una diversa pericolosità relativamente alla possibilità che malintenzionati possono avere di sfruttarla, e del danno che un tale sfruttamento può portare all'operatore.
Nel rapporto di prova, quindi, le vulnerabilità vengono aggregate e classificate in base al rischio che pongono all'operatore dai diversi punti di vista: gravità intrinseca della vulnerabilità, tipologia di informazioni potenzialmente accessibili al malintenzionato, tipologia di servizi potenzialmente soggetti a interferenza in caso di attacco, ecc.

5. Follow-up
L'operatore, una volta ricevuto il rapporto di prova, mette in atto le contromisure necessarie a eliminare le vulnerabilità riscontrate, o a ridurne la pericolosità, come indicato di seguito nel paragrafo "Utilizzo del rapporto di prova". Successivamente, su richiesta dell'operatore, il laboratorio di prova può tornare a eseguire una VA specificamente finalizzata a verificare l'efficacia delle contromisure adottate dall'operatore, così da fornire evidenza della eliminazione o riduzione dei rischi associati alle vulnerabilità che erano state evidenziate nelle fasi precedenti.

Durante l'audit di accreditamento Accredia richiede al laboratorio di dare dimostrazione pratica delle proprie modalità operative eseguendo le attività di prova oggetto di accreditamento, i VA.

Queste tipologie di test, come peraltro qualsiasi altra analisi o prova di laboratorio, i cui risultati sono sempre associati alla rispettiva incertezza di misura, non possono essere considerate completamente esaustive nella caratterizzazione di ogni possibile minaccia di tipo tecnologico che grava sui sistemi informatici degli operatori, in quanto la loro accuratezza ed efficacia dipendono da numerosi fattori.
Devono pertanto essere ripetute con una frequenza e una estensione idonea al sistema informatico e alle attività svolte: il piano delle prove da eseguire è stabilito dall'operatore stesso nell'ambito della propria valutazione dei rischi e della conseguente definizione dei "controlli operativi" da adottare per mitigarli.
L'adeguatezza del piano viene valutata dall'organismo di certificazione durante gli audit svolti presso l'operatore. L'accreditamento garantisce però che il laboratorio di prova sia dotato di personale competente per l'esecuzione dei test, che le prove vengano eseguite secondo i metodi dichiarati nel certificato di accreditamento e che le dotazioni strumentali (tools) impiegate dal laboratorio siano idonee e correttamente gestite.

Rapporto di prova
Al termine delle prove, il laboratorio rilascia all'operatore un rapporto di prova che elenca le eventuali vulnerabilità riscontrate, classificate per tipologia e gravità secondo gli standard previsti dai database internazionali sopra menzionati. I risultati sono relativi al perimetro (range di indirizzi IP) che è stato oggetto dei test e alla configurazione dei sistemi presente nel momento in cui i test sono stati eseguiti. La validità dei risultati non può quindi essere estesa, da parte del laboratorio, a istanti di tempo successivi a quelli nei quali è stato fatto il test, oppure a sistemi diversi da quelli sottoposti a prova.
Durante gli audit, sia quello di primo accreditamento che, soprattutto, nei successivi audit di sorveglianza (cfr. paragrafo 3.1.1), il gruppo di valutazione di Accredia esamina inoltre, a campione, i rapporti di prova precedentemente rilasciati dal laboratorio ai propri clienti.

Utilizzo del rapporto di prova
Una volta acquisito il rapporto di prova e analizzate le vulnerabilità riscontrate, l'operatore può:

- risolverle, mediante aggiornamento (patching) dei sistemi o loro sostituzione con altri che non ne siano affetti;

- accettare la presenza di alcune vulnerabilità, se il costo della loro risoluzione è troppo elevato rispetto al rischio che esse pongono, oppure di annullarle o mitigarle mediante delle contromisure, ad esempio implementando meccanismi che impediscano o limitino la possibilità di effettivo sfruttamento delle vulnerabilità, o cambiando le modalità di accesso/utilizzo del sistema;

- utilizzare le informazioni contenute nel rapporto di prova per trarre conclusioni di ordine più generale, soprattutto paragonando i risultati di test eseguiti a distanza di tempo l'uno dall'altro, ad esempio l'operatore può ridurre o aumentare l'estensione o la frequenza dei test.

La verifica di accreditamento viene svolta con l'ausilio di apposite checklist, sulle quali il gruppo di valutazione registra le evidenze osservate che comprovano la conformità ai requisiti, oppure le deviazioni dai requisiti. Al termine della verifica, la procedura di accreditamento continua come descritto al paragrafo 3.1.1.

3.5 Regolamento UE 910/2014 (eIDAS)

Come illustrato nella sezione 2.3.1, a livello europeo è stato emanato il Regolamento per l'identità digitale e i servizi fiduciari (es. la firma elettronica e le raccomandate elettroniche) denominato eIDAS, electronic Identification and Trust Services. eIDAS contiene le specifiche per l'utilizzo di mezzi di identificazione elettronica e servizi fiduciari da parte di cittadini, imprese e Pubbliche Amministrazioni per accedere ai servizi on line.
I soggetti che offrono servizi di identità elettronica e servizi fiduciari devono, a loro volta, possedere idonea certificazione per permettere agli utilizzatori di riporre fiducia in questi strumenti e nelle organizzazioni che li sviluppano e li gestiscono.

3.5.1 Riferimenti normativi

- **UNI CEI EN ISO/IEC 17065:2012** (norma di accreditamento)
  "Requisiti per organismi che certificano prodotti, processi e servizi".

- **ETSI 319 403-1 V.2.3.1.** (norma di accreditamento)
  Norma specifica per l'accreditamento degli organismi di valutazione della conformità operanti in ambito fiduciario, che integra di fatto la UNI CEI EN ISO/IEC 17065 per l'accreditamento degli organismi di certificazione di prodotti e servizi.

A seguire, per la valutazione dei Trust Service Providers (TSP):

- ETSI EN 319 401;
- ETSI EN 319 411-1;
- ETSI EN 319 411-2;
- ETSI TR 119 411-4;
- ETSI EN 319 421 e 422;
- ETSI EN 319 412 (parti 1, 2, 3, 4 e 5) ;
- ETSI EN TS 119 403-2;
- ETSI EN TS 119 403-3;
- ETSI EN 319 521 e ETSI EN 319 531;
- ETSI EN 319 522 e ETSI EN 319 532;
- ETSI TS 119 511;
- ETSI TS 119 441 ed ETSI EN 319 102-1;
- ETSI TS 119 612 e ETSI TS 119 615.

A seguire le Linee Guida che gli organismi di valutazione della conformità e i TSP debbono considerare nel loro operato:

- Assessment of Standards related to eIDAS - dicembre 2018;
- eIDAS: Overview on the implementation and uptake of Trust Services - gennaio 2018;
- Recommendations for QTSPs based on Standards - Technical Guidelines on trust services - dicembre 2017;
- Guidelines on Supervision of Qualified Trust Services - Technical Guidelines on trust services - dicembre 2017;
- Guidelines on Initiation of Qualified Trust Services - Technical Guidelines on trust services - dicembre 2017;
- Conformity assessment of Trust Service Providers - Technical Guidelines on trust services - dicembre 2017;
- Security framework for Trust Service Providers - Technical Guidelines on trust services - dicembre 2017;
- Security Guidelines on the appropriate use electronic signatures - giugno 2017;
- Security Guidelines on the appropriate use electronic seals - giugno 2017;
- Security Guidelines on the appropriate use electronic time stamps - giugno 2017;
- Security Guidelines on the appropriate use website authentication certificates - giugno 2017;

- Security Guidelines on the appropriate use of qualified electronic registered delivery services - giugno 2017;
- Auditing Framework for TSPs - aprile 2015.

3.5.2 Il razionale dell'accreditamento e della certificazione

Il Regolamento eIDAS, all'art. 3, punto 18, introduce il ruolo degli "organismi di valutazione della conformità" ai sensi del Regolamento 765/2008. Questi debbono essere accreditati secondo tale regolamento come competenti a effettuare valutazioni sui prestatori di servizi fiduciari.
Al successivo art. 20 viene introdotto il requisito secondo il quale i prestatori di servizi fiduciari debbono farsi valutare, a proprie spese, con una frequenza minima di 24 mesi, ai fini di confermare la soddisfazione dei requisiti individuati nel Regolamento eIDAS stesso. A fronte di questa previsione, al fine di garantire l'idoneità di un organismo a operare nell'ambito dei servizi fiduciari e, pertanto, per garantirne l'idoneità a valutare i prestatori di tali servizi, servivano delle regole non meglio specificate nel Regolamento. Pertanto, immediatamente dopo la pubblicazione del Regolamento, EA ha definito il set di norme applicabili alla fattispecie. Si tratta di norme elaborate dall'European Telecommunication Standard Institute (ETSI), uno dei tre Enti di normazione europei insieme al CEN e al Comitato Europeo di Normazione Elettrotecnica (CENELEC).

La domanda
I TSP sono chiamati a rispettare le indicazioni dell'AgID per l'attivazione del processo che li porterà a essere "qualificati" e, quindi, in grado di offrire servizi. Tali indicazioni si trovano nel Regolamento emanato dalla stessa Agenzia con la determinazione 185/2017. Tra i diversi adempimenti, nell'Allegato 2 si trova (§ g) la richiesta della valutazione di conformità rilasciata da un organismo di valutazione della conformità accreditato sulla base del Regolamento 765/2008. Il Regolamento richiede altresì la vigenza della certificazione di conformità alle norme tecniche internazionali ISO 9001 e ISO/IEC 27001, nella versione corrente al momento della presentazione della domanda, che coprano con il proprio campo di applicazione il perimetro fisico, logico e organizzativo di realizzazione dei propri servizi destinati a essere qualificati.

Il processo di certificazione
Alla ricezione della domanda di certificazione da parte di un TSP, l'organismo attiva un processo di pianificazione articolato, che tiene conto dei requisiti indicati dalla norma di accreditamento UNI CEI EN ISO/IEC 17065, integrata dalla ETSI EN 319 403-1, ma anche delle indicazioni delle Linee Guida citate precedentemente nei riferimenti normativi. Ovviamente, tutti i requisiti di legge sono obbligatori. La durata del ciclo di validità dei certificati è di 2 anni, con una sorveglianza annuale. Il secondo anno viene ripetuto integralmente il processo di valutazione iniziale, salvo alcune semplificazioni. L'organismo dovrà verificare che il TSP sia dotato di un'organizzazione adeguata al tipo di impegno derivante dai servizi erogati.
Gli auditor che fanno parte del team che svolge attività nello schema eIDAS sono qualificati secondo quanto richiesto dalla norma ETSI EN 319 403, che prevede, tra gli altri:

1. Titoli di studio accademici formali o formazione professionale o vasta esperienza che indichino la capacità generale di svolgere audit sulla base delle conoscenze richieste dallo schema;

2. Almeno 4 anni di esperienza pratica sul posto di lavoro a tempo pieno nella tecnologia dell'informazione, di cui almeno due anni con un ruolo o una funzione relativa a servizi fiduciari, e conoscenza:

   ❖ delle infrastrutture crittografiche a chiave pubblica;
   ❖ della sicurezza delle informazioni inclusa valutazione/gestione dei rischi;
   ❖ della sicurezza della rete e sicurezza fisica.

3. Conoscenza ulteriore di:

   ❖ principi, pratiche e tecniche di audit nel campo dei servizi fiduciari acquisiti in un corso di formazione di almeno cinque giorni;
   ❖ questioni relative alle varie aree dei servizi fiduciari, delle infrastrutture a chiave pubblica, della sicurezza delle informazioni inclusa la valutazione/gestione dei rischi, la sicurezza della rete e la sicurezza fisica;
   ❖ standard applicabili, le specifiche pubblicamente disponibili e i requisiti normativi per i TSP.

Questi requisiti completano le caratteristiche professionali che definiscono il profilo dell'auditor professionista. Partendo da competenze esistenti di base, è stato necessario attivare dei corsi di formazione e perfezionamento, proprio per la qualifica degli auditor "eIDAS", in una materia che richiede anche periodiche fasi di aggiornamento ed estensione delle competenze. Anche per gli aspetti commerciali, necessari all'acquisizione come clienti dei TSP, gli organismi hanno dovuto adeguare i propri processi e le competenze del personale addetto.
Una particolare attenzione è stata indirizzata alla verifica della sicurezza delle informazioni e della cybersecurity nella gestione delle infrastrutture cloud, prevedendo l'applicazione non solo della norma tecnica ISO/IEC 27001, già prevista dal Regolamento AgID, ma anche della norma ISO/IEC 27017, comprese le comunicazioni dedicate. In merito alle valutazioni sulla robustezza del sistema IT, che rappresenta l'infrastruttura tecnologica sulla quale si basa l'erogazione dei servizi fiduciari, sono state definite delle regole molto vincolanti, compresa l'adozione di un processo di gestione delle prove di vulnerabilità e penetrazione, cosiddette *Vulnerability Assessment - Penetration Testing (VA - PT)*, per le quali Accredia, primo Ente di accreditamento al mondo, ha sviluppato uno specifico schema di accreditamento per i laboratori.
Oggi, tali prove vengono eseguite con un livello di competenza e modalità ripetibili e con caratteristiche sottoposte a monitoraggio e valutazione da parte dello stesso Ente di accreditamento. Quanto sopra indica la verifica in termini generali, considerando che nella realtà un organismo presso un TSP svolge attività di audit su circa 1.000 requisiti, in un tempo che, a seconda dei servizi attivati e dei siti operativi può superare ampiamente le 24 se non 30 giornate di audit. Questo schema è stato ed è oggetto di confronto costruttivo con l'AgID. L'obiettivo di Accredia nel governare il processo di accreditamento è funzionale alla creazione di condizioni di massima affidabilità nelle certificazioni rilasciate sotto accreditamento.
Gli organismi accreditati, a loro volta, sono responsabili di verificare la sussistenza delle condizioni che migliorino la sicurezza ICT dei TSP "qualificati", al fine di assicurare, come in una filiera di monitoraggio, la più alta fiducia nei servizi "trusted" ai quali il mercato fa sempre più riferimento, in un continuo sviluppo del mercato digitale.

Le sorveglianze
Gli organismi sono chiamati a svolgere dei monitoraggi parziali, tra un audit completo e l'altro, sull'organizzazione, sull'infrastruttura (comprese le competenze delle risorse umane) e i servizi garantiti dai TSP. Queste verifiche sono svolte almeno una volta nell'arco dei 24 mesi (massimi) tra due audit completi, previsti dal Regolamento eIDAS. Durante gli audit intermedi, l'organismo può impiegare un solo auditor, se questi copre tutti gli aspetti di competenza sui servizi oggetto di valutazione. Anche il tempo di audit è sensibilmente ridotto, arrivando a essere tra un terzo e la metà del tempo di audit iniziale.

I rinnovi biennali
Come sopra indicato, il Regolamento eIDAS prevede che, su base biennale, vengano svolte delle attività di valutazione complete sui TSP; attività simili al processo iniziale di certificazione, salvo la possibilità di adire a una piccolissima riduzione di tempo, ove l'organismo rimanga lo stesso. Ciò deriva dal fatto che impiegando almeno uno degli auditor che già sono stati presso la stessa struttura, vi è una conoscenza pregressa che può rendere il processo di valutazione più fluido. Nella valutazione dei tempi di audit, si deve sempre tenere conto dei criteri di aumento e riduzione previsti dallo schema di ISMS (allegati alla norma tecnica ISO/IEC 27006 e AMD1). Questa riduzione, che Accredia richiede venga documentata in modo robusto, con appropriate evidenze e considerazioni, non può essere superiore al 20% del tempo massimo allocabile, ma non ha effetto sul calcolo dei tempi di audit delle sorveglianze.

Cosa aspettarsi
La sezione ha descritto certificazioni sui servizi e sulla sicurezza e cybersecurity di operatori di mercato, i TSP, che impattano in modo sostanziale sulla vita economica e sociale del Paese, ma anche dell'intera Unione europea. Appare evidente che tutto lo sforzo e l'impegno profuso per garantire il livello di qualità e, soprattutto, di sicurezza di tali servizi, ai fini della successiva "qualifica", processo che avviene in ambito regolamentato, è di livello critico proprio per la tenuta dell'intera infrastruttura digitale a servizio dell'economia nazionale e, per quanto applicabile al volume dei servizi non domestici, anche a quello dell'economia dell'Unione. Con questa consapevolezza e con la consapevolezza di come questi servizi si integreranno sempre più con le fasi dei "processi di Trattamento dei Dati Personali", specialmente con l'attivazione dei servizi REM e SERCQ (Recapiti Elettronici di Mail e di Servizi Postali in genere), l'opera di tutela della vasta infrastruttura ICT va letta in una prospettiva di valore che supera i confini nazionali e assurge a un livello di importanza strategica. Da qui l'impegno, la serietà richiesta a tutte le parti coinvolte, non ultimo a chi dovrà rendere il cittadino consapevole del contesto di vita digitale.

3.6 Data Protection Officer (DPO)

Come ultimo esempio di certificazione nel contesto di questa sintetica rassegna, si riportano le norme e i Regolamenti relativi alla certificazione delle persone chiamate a rivestire il ruolo di *Data Protection Officer* (DPO) così come definito dal GDPR descritto nella sezione 2.9.

3.6.1 Riferimenti normativi

- **ISO/IEC 17024** (norma di accreditamento)
  "Valutazione della conformità - Requisiti generali per organismi che eseguono la certificazione di persone";

- **UNI 11697**
  "Attività professionali non regolamentate - Profili professionali relativi al trattamento e alla protezione dei dati personali – Requisiti di conoscenza, abilità e competenza";

- **Prassi di Riferimento UNI/PdR 66:2019**
  "Raccomandazioni per la valutazione di conformità ai requisiti definiti dalla UNI 11697:2017 - Attività professionali non regolamentate - Profili professionali relativi al trattamento e alla protezione dei dati personali - Requisiti di conoscenza, abilità e competenza".

3.6.2 Contesto di riferimento

In Italia, partendo dal Regolamento UE 2016/679 (GDPR), al fine di definire le competenze di una figura centrale per sviluppare nelle organizzazioni un profilo di garanzia nella gestione dei dati, 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.
Nonostante la legislazione italiana non richieda specificamente la certificazione del personale, né quella dei sistemi, il carattere di volontarietà della certificazione di un Ente terzo rappresenta un'opportunità per quei professionisti che desiderano assicurare un elemento di garanzia al proprio profilo e per le aziende che devono scegliere un professionista cui affidarsi. Pur non avendo formalmente riconosciuto queste certificazioni, il Garante per la Protezione dei Dati Personali (GPDP) ha preso parte alle fasi di sviluppo della norma tecnica UNI 11697. Per un DPO, la certificazione UNI 11697, rilasciata da un organismo accreditato secondo la UNI CEI EN ISO/IEC 17024, è ritenuta una presunzione di competenza dei membri del gruppo di verifica quando certificano in ambito privacy.

3.6.3 Il processo di certificazione

La norma UNI 11697 e la Prassi di Riferimento UNI/PdR 66:2019 definiscono, rispettivamente, i requisiti e alcune raccomandazioni per la valutazione di conformità delle figure professionali che operano nel settore del trattamento e la protezione dei dati personali: DPO, Manager Privacy, Specialista Privacy, Valutatore Privacy. Nel seguito si farà riferimento, per una migliore comprensione dei requisiti di accesso e del processo che porta alla certificazione, a criteri definiti a titolo di esempio.

Requisiti
Al candidato che intende ottenere la certificazione come DPO vengono richiesti requisiti di accesso differenti in base all'apprendimento formale, non formale o informale di cui ha beneficiato:

1. Formale:

   a. laurea/laurea magistrale che includa discipline almeno in parte afferenti alle conoscenze del professionista privacy, legali o tecnico informatiche;
   b. diploma di scuola media superiore o laurea non afferente alle conoscenze del professionista privacy, legali o tecnico informatiche;

2. Non formale:

   a. corso di almeno 80 ore con attestazione finale avente per argomento la gestione della privacy e della sicurezza delle informazioni;
   b. qualora dei professionisti abbiano già seguito precedenti percorsi di formazione, non coincidenti con le indicazioni della norma UNI 11697, sarà cura dell'organismo di certificazione valutare analiticamente l'ammissibilità della formazione, assumendosi le responsabilità relative;

3. Informale:

   a. Il candidato deve dimostrare esperienza professionale nel settore della privacy. In particolare, sono richiesti:

      - minimo 6 anni di esperienza lavorativa legata alla privacy di cui almeno 4 anni in incarichi di livello manageriale;
      - se in possesso di laurea magistrale l'esperienza lavorativa si riduce a 4 anni di cui 3 in incarichi di livello manageriale;
      - se in possesso di diploma di scuola media superiore o laurea non afferente alle conoscenze del professionista privacy, legali o tecnico informatiche, minimo 8 anni di esperienza lavorativa di privacy di cui almeno 5 anni in incarichi di livello manageriale.

Esame

L'esame di certificazione si compone di 3 prove: due scritte e una orale. Nella prima prova scritta, vengono sottoposte al candidato 40 domande a risposta multipla, con 4 alternative. Le domande coprono gli elementi fondamentali di abilità e conoscenza previsti dalla norma UNI 11697. Il candidato ha a disposizione 80 minuti di tempo per svolgere la prova.
Nella seconda prova scritta vengono sottoposti 3 casi di studio volti a verificare l'attitudine, le abilità, le competenze e le conoscenze del candidato a gestire situazioni reali operative connesse al profilo oggetto di certificazione.
Ogni caso di studio presenta una situazione reale operativa per il quale saranno previsti più quesiti, a cui il candidato dovrà rispondere trattando il caso. Il tempo massimo a disposizione per lo svolgimento della prova è di 30 minuti. Nella prova orale, al candidato vengono sottoposte una serie di domande, al fine di indagare eventuali incertezze riscontrate nelle prove scritte e per approfondire il livello delle conoscenze acquisite dal candidato in tutte le aree previste dalla norma. Il tempo massimo a disposizione per lo svolgimento della prova è di 60 minuti.

La prova orale è suddivisa in:

1. approfondimento delle risposte errate delle due prove scritte;
2. discussione/simulazioni di situazioni reali operative (es. casi di studio, esercitazioni, role-play, ecc.) per valutare oltre alle abilità e alle competenze, anche le capacità personali;
3. analisi e discussione dell'elaborato di 1 dei 3 elaborati presentati in fase di iscrizione all'esame, frutto dell'esperienza professionale;
4. domande nell'ambito delle aree di conoscenze giuridica e tecnica;
5. domande per verificare la conoscenza dei concetti di "Privacy by Design", "Privacy by Default", tecniche di anonimizzazione, valutazione di impatto sulla protezione dei dati (DPIA), trattamento dei dati personali e relativi fattori di rischio.

L'accreditamento garantisce la competenza dell'organismo e la qualità del processo di certificazione del DPO. In particolare, in occasione della sessione d'esame, l'ispettore Accredia incaricato di effettuare verifica di valutazione del DPO deve accertare la competenza dell'esaminatore attraverso il curriculum vitae e con osservazione diretta (durante una sessione d'esame di certificazione), verificando come l'esaminatore conduce gli esami in termini di diligenza, prudenza e perizia. Viene inoltre valutata la documentazione dell'organismo di certificazione, in particolare verificando i prerequisiti per l'ammissione all'esame di certificazione del candidato, le modalità d'esame comunicate ai candidati e gli accordi contrattuali tra candidati e organismo di certificazione. Successivamente viene valutato l'esame orale relativamente alle tempistiche, al contenuto delle domande e alla valutazione delle risposte. In ultimo, l'ispettore Accredia verifica che i candidati siano stati esaminati con metodi di pari difficoltà e che siano state testate tutte le aree di competenza incluse nella norma UNI 11697 e nella Prassi di Riferimento UNI/PdR 66:2019.

Durata della certificazione, mantenimento e rinnovo

La certificazione ha una durata di 4 anni dalla data di delibera del certificato ed è soggetta a mantenimenti annuali; al termine del quadriennio è previsto il rinnovo del certificato. Annualmente, il professionista deve produrre e trasmettere all'organismo di certificazione le seguenti evidenze:

a) evidenza dell'esercizio retribuito della professione;

b) evidenza di aggiornamento professionale, tramite titoli di partecipazione ad attività di formazione, convegni, docenze, relazioni, gruppi di lavoro normativo o tecnico durante l'anno per almeno 16 ore all'anno;

c) un'autodichiarazione ai sensi degli artt. 46 e 76 del DPR 445/2000 contenente:

- le attività svolte durante l'anno, di cui al punto 1 rispetto ai punti 4 e 5 della norma UNI 11697, specifiche nel campo della protezione dati;
- l'elenco completo dei corsi di aggiornamento, partecipazione a convegni, seminari, relazioni e docenze inerenti agli argomenti relativi al settore della privacy come declinato nelle tabelle riepilogative per profilo;

- la presenza di reclami relativi all'attività certificata;
- la presenza di contenziosi legali in corso relativi all'attività certificata;
- evidenza della registrazione e del trattamento dei reclami ricevuti.

L'attività di sorveglianza può avere come esito il mantenimento, la sospensione o la revoca della certificazione accreditata a fronte della valutazione dell'organismo di certificazione in merito alla completezza e alla congruità della documentazione presentata, nonché alla gestione di eventuali reclami e/o contenziosi legali. Ai fini del rinnovo della certificazione dovranno essere presentate le stesse evidenze documentali richieste in fase di mantenimento e sorveglianza annuale; il professionista dovrà, in aggiunta, sostenere una verifica sul mantenimento delle competenze tramite un esame scritto.

3.7 Il ruolo di Accredia

Fin dal 2002, Accredia opera sia nell'ambito della sicurezza delle informazioni sia nell'ambito della cybersecurity. L'azione dell'Ente di accreditamento è esercitata sulla base delle previsioni normative dettate dal Regolamento europeo CE 765/08 [2.26].
All'interno del vasto dominio di azione, gli ambiti di competenza specifici 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, incluse le figure del DPO, dell'auditor GDPR e dell'auditor ISMS;
- le certificazioni di prodotto, processo e servizio, come quelle relative al sistema SPID e ai Regolamenti europei eIDAS e GDPR;
- le attività ispettive condotte a vari livelli, come le ispezioni su impianti e strutture;
- i laboratori di prova, con riferimento ai processi VA - PT.

L'esperienza di Accredia, in questo ambito, è particolarmente significativa. Alla data di settembre 2022 sono stati accreditati 20 organismi di valutazione della conformità per la sicurezza delle informazioni, 9 per la gestione dei servizi IT, 28 in ambito regolamentato (AgID), nonché 5 laboratori per VA.

4. Casi di studio

La certificazione delle capacità e competenze nell'ambito della cybersecurity è un tema sviluppato da molti anni, ma che continua a evolvere coerentemente con l'evoluzione delle minacce e delle migliori pratiche. In questo capitolo vengono riportati i risultati dell'analisi di una serie di casi di studio relativi a organizzazioni di diversa natura, che hanno intrapreso un percorso di certificazione legato alla cybersecurity. Per rendere i risultati utili a una platea più ampia possibile, la stessa si è limitata **a casi di certificazione dell'Information Security Management Systems (ISMS) secondo la norma tecnica ISO/IEC 27001 (e norme collegate appartenenti alla famiglia ISO 270XX)**. Un ISMS gestito correttamente rappresenta oggi un punto di partenza fondamentale per affrontare la complessità crescente degli scenari di attacco che organizzazioni pubbliche e private possono trovarsi a fronteggiare quotidianamente.
La norma ISO, pur nella sua complessità, è adattabile a casi caratterizzati da dimensioni e strutture organizzative diverse, con missioni, e quindi rischi, eterogenei e rappresenta un punto di riferimento a livello internazionale per tutti gli operatori per i quali la gestione del rischio cibernetico è un requisito imprescindibile.

Lo studio è stato indirizzato principalmente dai seguenti requisiti:

- comprendere le motivazioni che hanno portato le organizzazioni selezionate a intraprendere la strada della certificazione;
- identificare le possibili criticità che le organizzazioni hanno dovuto risolvere nella fase di adeguamento precedente alla certificazione;
- valutare gli effetti del processo di certificazione da diversi punti di vista: dalla riduzione del rischio legato alla cybersecurity agli aspetti di conformità rispetto alla normativa, fino agli effetti indiretti di carattere organizzativo e reputazionale.

Obiettivo complessivo, derivante in modo indiretto da questi requisiti, è quello di evidenziare cosa significhi per una organizzazione intraprendere la strada della certificazione dell'ISMS secondo la norma ISO/IEC 27001. Questo percorso per molte organizzazioni è spesso basato su una opportunità: un requisito imposto da un bando pubblico, una richiesta da parte di un fornitore importante, la necessità di allineare la qualità della propria offerta a quella della concorrenza, ecc.

Le motivazioni possono essere molte e molto diverse tra loro. Raramente, però, la scelta è basata su una conoscenza approfondita di come il percorso che si intraprende potrà cambiare profondamente la natura stessa dell'organizzazione, andando a impattare, positivamente, anche ambiti che non necessariamente saranno oggetto della certificazione.

4.1 Metodologia di indagine

L'analisi è partita dall'individuazione dei casi di studio, in numero limitato e in grado di rappresentare realtà differenti da diversi punti di vista. In particolare, si sono considerati i seguenti fattori:

- **Dimensione**: sono stati considerati casi di dimensione limitata, sia organizzazioni di grandi dimensioni, dato che il fattore dimensionale ha spesso un impatto sulla complessità e maturità dei processi di governo di una organizzazione. Comunemente, organizzazioni private di grandi dimensioni sono fortemente strutturate al loro interno, con funzioni ben definite, processi di controllo e meccanismi di verifica indipendenti.
  Al contrario, organizzazioni di piccole dimensioni hanno spesso un'organizzazione interna semplificata, con funzioni che vengono assegnate in modo fluido a un numero limitato di dipendenti, catene di comando di lunghezza ridotta, tutte caratteristiche che rendono queste strutture più facilmente adattabili per rispondere rapidamente alle mutazioni dei contesti in cui operano. Questa caratteristica ha un impatto forte sulla capacità dell'organizzazione di adattare la governance interna per rispondere a quanto richiesto dalla norma ISO.

- **Natura**: sono stati considerati soprattutto attori del mondo privato e una realtà controllata dal pubblico, per valutare se la natura dell'organizzazione ha un impatto significativo sul processo di certificazione.

- **Mercato**: sono stati selezionati casi di studio appartenenti ad ambiti di mercato anche molto diversi tra loro, per dimostrare come la certificazione di un ISMS trovi applicazione in contesti e per motivazioni molto specifiche e peculiari per ogni singola realtà. Alcune realtà hanno un mercato di riferimento molto preciso e su quello sono focalizzate. Altre realtà, tipicamente di maggiore dimensione, offrono prodotti e servizi in numerosi ambiti, anche molto eterogenei tra loro. Queste differenze impattano sulla complessità del sistema di gestione interno e, quindi, sull'ISMS, oggetto della certificazione.

- **Esperienza**: ultimo aspetto tenuto in considerazione nella fase di selezione è stata l'età della certificazione. Organizzazioni certificate da molti anni maturano tipicamente un'esperienza che permette di valutare nel modo migliore i vantaggi derivanti dall'aver intrapreso questo percorso, ma d'altra parte rende meno recente l'esperienza della fase di adeguamento pre-certificazione, fattore che invece è ben presente a chi ha ottenuto la stessa più recentemente.

Sulla base di questi fattori, è stata considerata una lista delle aziende italiane con una certificazione conforme alla norma ISO/IEC 27001 valida ad aprile 2022.

Sono stati estratti i candidati per sondarne la disponibilità a partecipare alla ricerca e infine sono state selezionate 4 organizzazioni:

- ***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 (al 30 giugno 2022) 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 Spa***
  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'indagine è stata svolta attraverso un'interlocuzione da parte di due esperti con il personale delle organizzazioni selezionate. A ciascuna organizzazione è stato chiesto, in via preliminare, di identificare le persone più adatte a interloquire sul tema. In molti casi le persone selezionate sono stati i responsabili della sicurezza IT (CISO, CIO, o similari).
Gli stessi sono stati in alcuni casi coadiuvati da altri responsabili di funzioni più specifiche (Responsabile sicurezza logica, responsabile per le certificazioni, etc.) la cui partecipazione è stata ritenuta utile per approfondire temi legati all'oggetto dell'indagine. L'indagine si è sviluppata per ogni caso attraverso due fasi:

1. **Erogazione del questionario**. Inizialmente è stato trasmesso all'interlocutore un questionario costituito da 19 domande a risposta aperta (cfr. sezione 4.3); a ogni organizzazione è stato chiesto di rispondere liberamente a ciascuna domanda, senza fornire ulteriori indicazioni riguardo all'interpretazione delle stesse e senza porre vincoli sulle risposte (es. limiti di lunghezza). Scopo del questionario è stato quello di fornire una base di informazioni uniforme tra i diversi casi oggetto di studio; una base che riuscisse a superare le differenze dovute all'eterogeneità dei casi considerati.

2. **Intervista**. In seconda fase sono state effettuate delle interviste presso l'organizzazione. L'intervista non è stata organizzata su uno specifico argomento; piuttosto, partendo dall'interpretazione data dagli intervistati alle domande del questionario, la stessa ha in molti casi spaziato su argomenti non direttamente legati al questionario, comunque riferibili al tema di questa indagine. Scopo delle interviste è stato quello di acquisire direttamente dalle organizzazioni coinvolte informazioni specifiche e aspetti generali riferibili alla loro esperienza sul tema certificazione ISO/IEC 27001, elementi che non sarebbe stato possibile codificare all'interno del questionario, permettendo quindi al team di identificare peculiarità proprie di ciascuna delle organizzazioni coinvolte nello studio. Le interviste si sono svolte tra maggio e giugno del 2022 e ogni intervista ha coinvolto le organizzazioni selezionate per una durata massima di due ore.

4.2 Questionario

Il contenuto del questionario condiviso con le organizzazioni è stato preparato dal gruppo di lavoro che ha identificato 19 domande divise in 3 gruppi.

4.2.1 Domande introduttive

Un primo insieme di 2 domande è stato dedicato a definire le basi su cui è stato affrontato il percorso di certificazione.

1. Quali sono state le motivazioni che hanno spinto la sua organizzazione a perseguire la certificazione ISO/IEC 27001?

Scopo della domanda è stato sondare gli obiettivi che l'organizzazione intervistata intendeva raggiungere quando ha iniziato il processo di certificazione. Le motivazioni che spingono a porsi questi obiettivi spesso divergono, anche sensibilmente, dalla percezione del ritorno che si ottiene dalla certificazione sul lungo periodo.

2. Qual è l'ambito della certificazione nell'organizzazione?

Uno degli aspetti fondamentali a cui devono porre attenzione le organizzazioni che intendono certificare il proprio ISMS secondo la norma ISO/IEC 27001, è la corretta definizione dell'ambito, ossia del perimetro che racchiude i dati, i servizi, e i sistemi oggetto della gestione tramite l'ISMS. Tale ambito può essere definito in modo molto diverso a seconda degli obiettivi che l'organizzazione si pone. È anche possibile che a seguito di un primo ottenimento della certificazione, l'organizzazione decida negli anni successivi di far crescere l'ambito di applicazione, con un approccio incrementale che includa nel tempo un numero sempre maggiore di elementi.

4.2.2 Domande sulla complessità della fase di adeguamento

La fase di certificazione prevista per la norma ISO/IEC 27001 è in realtà solo l'ultimo passo del processo. A monte di questa fase, l'organizzazione interessata alla certificazione deve tipicamente svolgere una attività di adeguamento dei propri sistemi informativi e dei processi attraverso cui la

sicurezza delle informazioni viene gestita, per allineare gli stessi a quanto previsto dalla norma ISO. Questa fase di adeguamento può essere più o meno complessa e lunga, dipendentemente da molteplici fattori (es. la dimensione dell'ambito, il livello di maturità dell'organizzazione nella gestione della sicurezza informatica, il livello di preparazione dei dipendenti, ecc.) e può quindi avere un impatto importante, anche dal punto di vista economico, sull'organizzazione.

3. Nel processo di adeguamento che ha portato all'ottenimento della certificazione, in che modo hanno impattato le regolamentazioni che insistono sul settore di riferimento in cui opera la sua organizzazione?

Negli ultimi anni è entrato in vigore un numero crescente di regolamentazioni che impattano in modo spesso diretto la sicurezza delle informazioni e dei sistemi IT. Alcune di queste regolamentazioni hanno carattere generale, altre sono invece prettamente settoriali (cfr. capitolo 2 per una panoramica). Tali regolamenti possono essere parte delle motivazioni per chi intraprende il percorso di certificazione e, tipicamente, il loro contenuto impatta la fase di adeguamento.

4. Nel processo di adeguamento che ha portato all'ottenimento della certificazione, in che modo hanno impattato eventuali considerazioni relative al contesto interno ed esterno in cui opera l'organizzazione (es. dimensione e struttura della supply chain, applicazione dei prodotti in un contesto critico e/o normato, ecc.)?

Le organizzazioni moderne sempre più raramente lavorano in un contesto di isolamento; al contrario sono parte integrante di un complesso ecosistema di produttori ed erogatori di servizi. Questo ecosistema può avere un impatto fondamentale sul processo di certificazione, potendo rappresentare l'origine di un requisito di conformità oppure offrendo l'opportunità di un vantaggio competitivo.

5. Nel processo di adeguamento che ha portato all'ottenimento della certificazione, sono stati identificati punti della norma rispetto ai quali un adeguamento è stato maggiormente difficoltoso?

L'adeguamento alla norma ISO/IEC 27001 tocca numerosi aspetti legati alla gestione della sicurezza delle informazioni. L'adeguamento dei processi interni rispetto ad alcuni di questi aspetti può richiedere uno sforzo importante. Tali criticità, se identificate per tempo, possono rappresentare un punto di attenzione su cui concentrare gli sforzi dell'organizzazione.

6. In merito all'organizzazione aziendale, in che modo il processo di certificazione ha impattato imponendo modifiche o aggiornamenti (es. integrazione all'organigramma, identificazione di nuove funzioni operative, ecc.)?

Non sempre la struttura organizzativa della realtà che affronta il percorso di certificazione è coerente con quanto indicato dalla norma ISO/IEC 27001. Adeguamenti dell'organizzazione possono a volte essere necessari, portando a modifiche anche importanti della stessa. Tali adeguamenti possono risolversi nell'identificazione di nuove funzioni e ruoli, o richiedere interventi più importanti di integrazione dell'organigramma con modifiche sostanziali alle catene decisionali.

7. In merito alle competenze tecniche nell'ambito della sicurezza dei sistemi informatici, il processo di certificazione ha richiesto l'assunzione di nuovo personale qualificato o il ricorso a servizi di consulenza esterna specialistica?

La norma ISO/IEC 27001 e i relativi documenti forniscono indicazioni che non si limitano a toccare solamente gli aspetti di governo della sicurezza, ma richiedono adeguamenti anche alle infrastrutture tecniche. Tali adeguamenti, in cascata, possono imporre l'acquisizione di personale specializzato o la riqualificazione di personale già in forze all'organizzazione.

8. In merito alla consapevolezza del personale rispetto ai rischi cyber, quali azioni ha intrapreso la sua organizzazione per adeguarsi a quanto richiesto dalla norma? In che modo è stata misurata l'efficacia di tali azioni?

Uno degli aspetti cruciali su cui oggi si combattono le battaglie per la sicurezza dei sistemi informatici è sicuramente il fattore umano: al crescere del livello di complessità delle soluzioni tecnologiche per la protezione dei sistemi e delle informazioni, sempre più spesso l'anello debole risulta essere l'uomo, vittima di sofisticati attacchi basati su social engineering. La norma ISO correttamente pone una forte attenzione al problema richiedendo che il personale dell'organizzazione sia adeguatamente reso consapevole dei rischi insiti nell'uso di tecnologie e sistemi connessi, e delle responsabilità che da quest'uso derivano.

9. In merito alla formazione del personale sui temi della cybersecurity, quali azioni ha intrapreso la sua organizzazione per adeguarsi a quanto richiesto dalla norma? In che modo è stata misurata l'efficacia di tali azioni?

Laddove la consapevolezza dei rischi è un aspetto che deve toccare tutto il personale dell'organizzazione, elementi specifici devono essere oggetto di formazione più puntuale sui temi della cybersecurity, formazione che li aiuti a diventare parte integrante dell'ISMS.

4.2.3 Domande sugli effetti della certificazione

Questo insieme di domande conclusive mira a identificare i risultati tangibili che le organizzazioni intervistate hanno potuto identificare a valle della certificazione.

10. La sua organizzazione ha valutato la riduzione del rischio cyber a valle del processo di certificazione? È stato possibile misurare una diminuzione del numero di incidenti subiti? È stata osservata una diminuzione dell'impatto di ciascun incidente?

L'adozione di un ISMS ha tra i suoi obiettivi anche (ma non solo) la riduzione del rischio legato al verificarsi di incidenti ascrivibili ad attacchi informatici. Tale diminuzione del rischio dovrebbe tradursi in una diminuzione del numero di incidenti (a causa di un maggiore consapevolezza e un migliore processo di prevenzione) e del relativo impatto (a causa di una maggiore capacità di risposta e confinamento degli incidenti). È importante però specificare che questa correlazione, ovvia a livello intuitivo, non è mai diretta, e non sempre è facilmente misurabile.

11. La sua organizzazione ha misurato una riduzione dei tempi di risposta a seguito di incidente derivante dal miglioramento dei processi di gestione della sicurezza imputabile al percorso di certificazione?

Un aspetto che è invece più direttamente misurabile e ascrivibile a un ISMS è la riduzione dei tempi di risposta agli incidenti. La definizione di processi di risposta ben definiti, monitorati e valutati, aiuta le organizzazioni a essere pronte e reattive nel momento in cui un incidente si verifica.

12. In che misura il processo di certificazione ha determinato vantaggi in termini organizzativi, rispetto all'eventuale reingegnerizzazione di processi, al miglioramento della capacità dell'organizzazione di gestire i propri asset e alle relazioni con i fornitori?

La vita di ogni organizzazione, anche di dimensione piccola, è basata sulla capacità dei suoi responsabili di definire dei processi di funzionamento efficaci e adatti alla sua specifica realtà.
La certificazione dell'ISMS, secondo la norma ISO/IEC 27001, richiede frequentemente una revisione e, in alcuni casi, una reingegnerizzazione di alcuni di questi processi.
Tale revisione è un'occasione importante per puntare a un maggiore efficientamento dei processi stessi.

13. In che misura il processo di certificazione ha determinato vantaggi in termini di conformità normativa? È possibile misurare una riduzione della possibilità di sanzioni determinate da violazione di conformità? È migliorata la capacità dell'organizzazione, anche attraverso l'adozione di strumenti software, di gestire e monitorare la conformità?

Per tutte le organizzazioni, la conformità normativa è un aspetto fondamentale. In alcuni settori il numero di regolamenti che impongono requisiti sulla gestione dei sistemi informativi, anche dal punto di vista della sicurezza, può essere molto elevato. L'adozione di un ISMS certificato solitamente semplifica la gestione della conformità, in quanto fornisce un modello di gestione dei processi che, essendo coerente con le best practice di settore, incontra facilmente i requisiti imposti dalle norme di riferimento.

14. In che misura il processo di certificazione ha determinato vantaggi in termini di riduzione dei premi assicurativi per eventuali polizze inerenti al rischio informatico?

La gestione della cybersecurity, basata sull'analisi del rischio, rappresenta l'approccio oggi più usato da organizzazioni di ogni settore. Con questo approccio, l'obiettivo dell'organizzazione non è direttamente quello di rendere sicuri i propri sistemi e i propri dati, piuttosto di ridurre, a un livello tollerabile, il rischio che gli stessi siano oggetto di un incidente dovuto a un attacco. Il rischio residuo che non può essere ulteriormente mitigato è di frequente oggetto di una apposita copertura assicurativa. La corretta gestione di un ISMS, aiutando a diminuire questo rischio, può portare, laddove le condizioni lo consentano, a una riduzione dei relativi premi assicurativi.

15. In che misura il processo di certificazione, e in particolare le azioni volte alla gestione del rischio, hanno impattato sulla capacità dell'organizzazione di analizzare i costi?

Uno dei grandi vantaggi dell'adozione di un ISMS ben strutturato è la capacità dell'organizzazione di poter monitorare e valutare l'efficienza dei processi, portando a una maggiore capacità di valutazione dei costi e una più semplice identificazione delle opportunità di miglioramento.

16. In che misura il processo di certificazione ha determinato il miglioramento della qualità delle attrezzature hardware e software e delle infrastrutture IT dell'organizzazione?

Durante il processo di adeguamento, non è infrequente che si presentino delle importanti opportunità di miglioramento del supporto tecnologico ai processi di gestione della sicurezza delle informazioni.

17. In che misura la certificazione ha incrementato le possibilità dell'organizzazione di partecipare a bandi di gara pubblici o privati?

Sempre più spesso bandi di gara pubblici, ma anche opportunità di collaborazione tra privati, sono accessibili solo dimostrando una corretta gestione dei processi di gestione della sicurezza applicata ai sistemi IT. La certificazione, da questo punto di vista, può costituire un fattore abilitante importante.

18. In relazione all'adozione della certificazione, è stato possibile identificare un miglioramento reputazionale dell'organizzazione nei confronti di clienti, eventuali azionisti, parti sociali, partner o altri stakeholder?

Il fatto che negli ultimi anni gli incidenti informatici e i data breach siano diventati così pervasivi e impattanti, li ha portati alla ribalta dell'opinione pubblica. Se questo può rappresentare un aspetto positivo, dal punto di vista della consapevolezza generale, rappresenta anche un rischio reputazionale importante per le organizzazioni. Da questo punto di vista la certificazione viene spesa sempre più spesso come attestazione indipendente del livello di qualità dei servizi offerti dalle organizzazioni certificate.

19. In che misura il processo di certificazione ha determinato vantaggi in termini di risorse umane, in relazione a una maggiore consapevolezza del personale (non solo circa i rischi cyber, ma in generale circa il proprio contesto) e a una migliore identificazione e controllo delle responsabilità?

In generale, il processo di certificazione impone una crescita di tutto il personale dell'organizzazione dal punto di vista della consapevolezza dei rischi, ma soprattutto dal punto di vista delle responsabilità dei singoli rispetto alla sicurezza dell'intera organizzazione.

4.3 Analisi dei casi

Per ogni caso viene riportata, a valle di una breve introduzione alla realtà oggetto di studio, un'analisi dei punti salienti emersi dalle risposte al questionario e di quanto discusso nella successiva intervista. L'analisi non può essere estensiva su quanto riportato nel questionario, ma ha l'obiettivo di evidenziare le peculiarità di ogni caso.

4.3.1 Gruppo BCC ICCREA

Il Gruppo BCC Iccrea si è costituito il 4 marzo 2019 nell'ambito della Riforma del Credito Cooperativo italiano (Legge 49/2016 e successive modifiche) che ha previsto l'obbligo per tutte le Banche di Credito Cooperativo (BCC) di aderire a un Gruppo Bancario Cooperativo. Figura nuova nel panorama bancario italiano ed europeo, il Gruppo ha raccolto l'eredità di oltre 50 anni di storia della Capogruppo Iccrea Banca. Quest'ultima nasce il 30 novembre del 1963, quando i rappresentanti di 190 Casse Rurali si riuniscono a Roma per stipulare l'atto costitutivo dell'Istituto di Credito delle Casse Rurali e Artigiane (CRA) con lo scopo di far crescere l'attività delle CRA, agevolandone e coordinandone l'azione attraverso lo svolgimento di funzioni creditizie, l'intermediazione bancaria e l'assistenza finanziaria. Le Casse Rurali e Artigiane diventano le attuali BCC con il Testo Unico delle leggi in materia bancaria e creditizia, detto anche Testo Unico Bancario (TUB), emanato con il D.Lgs. 385/1993. Il TUB segue la strada comunitaria intrapresa con il D.Lgs. 481/1992 e conferma il superamento della specializzazione delle Casse Rurali e Artigiane nell'agricoltura e nell'artigianato (incompatibile con un'efficiente gestione dell'impresa bancaria), cancellando i limiti di governance e di operatività e consentendo alle nuove BCC di avere nella propria compagine sociale non più solo agricoltori e artigiani e di offrire tutti i servizi e i prodotti finanziari al pari delle altre banche. In particolare il Gruppo si costituisce con l'adesione di 142 BCC che sottoscrivono, insieme alla Capogruppo Iccrea Banca, il contratto di coesione. Come previsto dal contratto di coesione, il Gruppo BCC Iccrea ha l'obiettivo di rafforzare la stabilità delle Banche Aderenti, di agevolare il conseguimento di livelli di efficienza adeguati ai mercati di riferimento, il rispetto delle Disposizioni di Vigilanza, nonché di favorire lo sviluppo dei Soci e delle comunità locali in cui operano, la cooperazione e l'educazione al risparmio e alla previdenza, nonché la coesione sociale e la crescita responsabile e sostenibile dei territori di insediamento.
BCC Banca Iccrea, nell'ambito delle strategie di gestione del rischio del Gruppo BCC Iccrea, ha intrapreso da tempo un percorso diretto a innalzare le capacità di cyber sicurezza e di "operational resilience" ovvero quelle capacità funzionali a intercettare e gestire eventi cyber e di sicurezza che possano avere effetti non trascurabili sulla vita aziendale e del Gruppo, nonché sulla relazione con gli stakeholder. Nell'ambito di tale percorso, la chiara identificazione delle esigenze di tutela e protezione delle informazioni complessivamente trattate, per mezzo della progettazione e implementazione di adeguati livelli di "sicurezza" e di "continuità del servizio", costituisce un obiettivo imprescindibile. L'operare in un mercato regolamentato come quello finanziario, che prevede l'identificazione e la gestione degli aspetti di rischio associabili a ogni iniziativa aziendale, ha richiesto al Gruppo di approcciare subito in modo sistematico le tematiche, complesse e pervasive, come quella della cyber sicurezza e della "operational resilience". In questo percorso, BCC Banca Iccrea ha chiaramente identificato sin da subito i driver di intervento, quali l'Organizzazione, i Processi e le Tecnologie; ciò rende evidente come l'approccio elaborato da BCC Banca Iccrea e dal Gruppo al tema della cyber sicurezza e della operational resilience non sia confinato entro un ambito meramente tecnologico: al contrario, gli ambiti organizzativi e di processo, che includono anche i profili relativi alle risorse umane, rivestono un ruolo centrale per la

“messa a terra” sin da subito di modelli operativi efficaci e in grado di rimodularsi in modo veloce ed efficiente in dipendenza delle evoluzioni del contesto esterno (es. nuove minacce cyber, ecc.) e/o di quello interno (es. modifiche di processi operativi, riorganizzazioni interne, ecc.).
Nel perseguire tale approccio, BCC Banca Iccrea ha rilevato l’esigenza, per consentire un rapido set up dei framework di sicurezza delle informazioni e continuità operativa, di identificare riferimenti ulteriori rispetto alle prescrizioni normative di settore, identificando e adottando “riferimenti” che fossero già consolidati sul mercato e nel settore di riferimento, al fine di rendere riconoscibile, non solo internamente a BCC Banca Iccrea e indirettamente per il Gruppo, il percorso avviato e gli obiettivi raggiunti. Nell’identificare e selezionare questi “riferimenti” sono stati individuati quelli che gli stakeholder, inclusi gli Organismi di Vigilanza di settore, avrebbero potuto apprezzare in termini di risultati raggiunti, oltre che per il commitment del board e per l’impegno delle strutture operative.
Da qui la decisione di adottare, dopo attenta analisi, la norma ISO/IEC 27001 (congiuntamente alla norma ISO 22031) come framework di riferimento per il governo complessivo e integrato delle tematiche legate alla cyber sicurezza e alla operational resilience, nonché come baseline di riferimento per lo sviluppo delle Politiche di Gruppo in tema di Sicurezza delle Informazioni e continuità operativa. Oltre a adottare tali standard ISO, BCC Banca Iccrea, a partire dal 2009, ha deciso di sottoporre i due sistemi di gestione (ISO/IEC 27001 e ISO 22031) al vaglio di un terzo soggetto indipendente. Tale ulteriore evoluzione è stata prevista al fine di garantire alle strutture interne responsabili dello sviluppo sia dei sistemi di gestione della Capogruppo che delle Politiche di Gruppo, che da essi ne derivano, di fruire dei benefici di una periodica attività di challenge e verifica della efficace implementazione e del regolare esercizio di quanto definito, tramite una expert opinion rilasciata dai professionisti indipendenti di un organismo di certificazione.
Quanto esposto in sintesi evidenzia come i sistemi di gestione di BCC Banca Iccrea, certificati a norma ISO 22301 e ISO/IEC 27001, siano oggi sia un elemento distintivo per la Capogruppo che un asset importante nell’ambito dei processi di governance del Gruppo nel suo complesso, costituendo una importante “matrice” a partire dalla quale sviluppare e far evolvere i framework di Gruppo in tema di sicurezza delle informazioni e continuità operativa. La linea guida rappresentata dal ISMS ed il percorso di certificazione messo in atto da BCC Banca Iccrea, rappresentano per il Gruppo anche strumenti importanti per governare quelle funzioni che sempre più hanno rilevanza nell’ambito della cybersecurity. Inoltre, in tema di conformità normativa, fattore fortemente caratterizzante il settore finanziario, l’adozione del ISMS supporta l’esigenza, spesso anticipata, di adozione delle migliori prassi previste nelle evoluzioni normative di settore; indirettamente, quindi, supportando il change management dell’organizzazione nell’affrontare i cambiamenti preparando per tempo l’organizzazione al momento in cui queste novità si consolideranno anche attraverso l’attività del legislatore. La chiara identificazione delle aree di presidio del controllo realizzata per mezzo del ISMS (IT, rischi informativi, continuità operativa, etc.) costituisce un efficace meccanismo di supporto alla identificazione degli elementi di novità normativa quando questi sono ancora in fase di definizione, consentendo di importarli rapidamente e in modo efficace all’interno del ISMS. Altro ambito significativo positivamente impattato dall’adozione di un ISMS certificato è quello inerente alla gestione dei profili di sicurezza nell'acquisizione dei servizi e beni da terze parti, sia nella fase di selezione del fornitore, che nella fase di selezione della singola fornitura. In tale ambito, l’ISMS è stato abilitante nel perseguire l’obiettivo di “estendere” alla relazione con le terze parti gli obiettivi di sicurezza definiti dal Gruppo nell’ambito delle proprie Politiche di information security management.

4.3.2 Poste Italiane

Con 160 anni di storia, una rete di circa 12.800 uffici postali, 121.000 dipendenti, 586 miliardi di euro di attività finanziarie totali e 35 milioni di clienti, il Gruppo Poste Italiane rappresenta una realtà unica all'interno del nostro Paese. Il gruppo costituisce la più grande rete di distribuzione di servizi in Italia, attiva in numerosi settori, dalla logistica e consegna di corrispondenza e pacchi, i settori che più tradizionalmente sono associati al brand, ai servizi finanziari e assicurativi, tramite le società BancoPosta e PosteVita, ai sistemi di pagamento e servizi di telefonia tramite la società Postepay. L'Azienda riveste un ruolo importante nel Paese, dando un forte contributo alla filiera produttiva e all'economia nazionale, generando risultati positivi attraverso il proprio business, ma anche generando esternalità tramite l'attivazione di una catena di fornitura locale.
La sicurezza delle informazioni ha acquisito nel tempo un ruolo sempre più importante per Poste italiane fino a rappresentare un elemento distintivo e caratterizzante sia l'azienda sia tutti i servizi erogati. La tradizionale fiducia riposta dai clienti nei prodotti venduti tramite il canale fisico degli uffici postali si è generalmente trasformata, nel tempo, in affidabilità e fiducia nei confronti dell'azienda e dei prodotti e servizi emessi, inclusi i prodotti digitali. È risultato pertanto essenziale dotarsi di un ISMS, limitato inizialmente al perimetro delle funzioni tecnologiche ICT e sicurezza informatica, ma che nel tempo è stato esteso a tutta l'azienda, al fine di poter garantire una adeguata governance e una corretta attuazione di tutte le misure, sia organizzative sia tecnologiche. Il riconoscimento da parte di un ente terzo indipendente della maturità dei processi interni ha dato a Poste Italiane l'impulso per dotarsi di un Sistema di Gestione Integrato (SGI) conforme e certificato su vari schemi normativi di riferimento: "Qualità verso il Cliente" (ISO 9001:2015), "Gestione Servizi Informatici" (ISO/IEC 20000-1:2018) e "Sicurezza delle Informazioni" (ISO/IEC 27001:2013). La scelta strategica di certificare il SGI "Servizi ICT e Sicurezza Informatica" è scaturita inizialmente da un approccio di tipo volontario da parte dell'azienda; tuttavia, nel corso degli anni è divenuto un fattore abilitante a supporto del business di Poste Italiane. Infatti, lo sviluppo del SGI e il mantenimento delle relative certificazioni rappresentano:

- un requisito cogente richiesto dall'AgID per l'accreditamento di Poste Italiane quale gestore delle identità digitali a livello nazionale (SPID) e di altri importanti servizi fiduciari qualificati ai sensi della normativa europea (eIDAS);
- un requisito essenziale per la partecipazione a gare d'appalto della Pubblica Amministrazione e di Grandi Clienti, che ormai richiedono le certificazioni del fornitore in conformità alle migliori pratiche internazionali di riferimento;
- un fattore esimente e di garanzia verso Istituzioni e Organi di Controllo ai quali Poste Italiane è soggetta, nell'ambito degli adempimenti correlati all'erogazione dei servizi;
- un fattore distintivo per l'immagine dell'azienda verso gli stakeholder e, in particolare, verso gli investitori.

Il campo di applicazione su cui è stato costruito SGI è molto articolato e comprende tutti i "Servizi ICT e Sicurezza Informatica" gestiti da Poste Italiane. Gli ambiti delle certificazioni sono stati oggetto (nel tempo e in modo incrementale) di estensione territoriale, organizzativa e funzionale. L'ambito di applicazione è pertanto un perimetro dinamico, che annualmente viene aggiornato secondo lo sviluppo organizzativo aziendale e/o dell'evoluzione cui sono oggetto i servizi erogati ai clienti. Ad esempio, è stato dato l'avvio alla pianificazione delle certificazioni anche per l'ambito cloud, seguendo quanto previsto dagli standard ISO/IEC 27017 e 27018.

L'implementazione del SGI è iniziata con un lavoro preliminare di identificazione e mappatura di tutte le normative applicabili e i relativi vincoli che le stesse impongono attraverso la prescrizione di requisiti (di conformità e sicurezza) che in alcuni casi risultano essere molto più stringenti rispetto a quanto normalmente viene richiesto dalla norma 27001.
Tale attività è comunque sempre in corso, in modo da poter mantenere il SGI sempre allineato rispetto ai requisiti di conformità nazionali e internazionali. Nella successiva fase di adeguamento, un passaggio che ha richiesto particolare attenzione, e che ha impattato in modo più forte la struttura di governo interna, è stata l'implementazione di un approccio alla gestione basata sul rischio e, in particolare, la responsabilizzazione rispetto al concetto di rischio residuo.
In merito alla formazione del personale, l'approccio sistematico della certificazione rende normalmente evidenti eventuali lacune relative alle competenze, allo sforzo profuso e al livello di capacità che l'organizzazione deve avere per affrontare determinati tipi di attività o di servizi. Il processo di certificazione rende, da un lato, necessario formare le persone interne in modo continuativo (in alcuni casi anche avviare dei processi di riconversione), dall'altro lato rende evidente la necessità di reperire le competenze e le capacità necessarie non presenti nell'organizzazione, anche attraverso consulenza specialistica esterna. Relativamente agli impatti positivi, l'introduzione dei processi di certificazione per tutti i servizi ICT e dei servizi di sicurezza informatica permette senz'altro di migliorare il profilo di protezione, la resilienza e la capacità di prevenire incidenti di sicurezza sia interni che esterni, ma non permette di abbattere il numero degli attacchi subiti. L'attività sistematica e ordinata di certificazione permette quindi di migliorare la prevenzione e la capacità di risposta, anche organizzativa, ma non può direttamente impattare la frequenza o la numerosità degli incidenti di sicurezza informatica, che dipendono, più in generale, dal profilo e dalla numerosità crescente delle minacce, più che dall'organizzazione. Forse l'impatto maggiore derivante dalla certificazione viene identificato da Poste Italiane nell'accrescimento della cultura aziendale. Tutte le risorse umane coinvolte nel processo di certificazione hanno incrementato significativamente la propria consapevolezza circa il contributo del lavoro alla maggiore sicurezza dell'azienda. Infatti, il processo di certificazione permette di avere una maggiore visibilità incrociata del proprio ruolo rispetto a quello degli altri, oltre che delle interrelazioni tra le varie componenti aziendali. Pertanto, i vari momenti previsti dalle attività di certificazione, in particolare i momenti cruciali relativi al Riesame della Direzione (che coinvolge il management) e all'Exit Meeting (che coinvolge generalmente tutti i soggetti interni e le funzioni coinvolte nel percorso di certificazione, inclusi gli auditor esterni), rappresentano dei momenti di accrescimento della consapevolezza e sensibilizzazione per tutta l'organizzazione. Si prende coscienza dei punti di forza e dei punti di miglioramento, sui quali poi si lavorerà nei mesi successivi per la risoluzione o il miglioramento dei servizi e dell'azienda.

4.3.3 Atac SpA

Atac SpA è l'azienda controllata al 100% da Roma Capitale che gestisce la maggior parte delle forme di mobilità collettiva dell'area metropolitana di Roma: mezzi di superficie, metropolitane e ferrovie (Termini - Centocelle) fino alla gestione dei parcheggi di scambio e della sosta tariffata su strada. Atac ha recentemente iniziato a guardare il proprio patrimonio informativo e informatico in un'ottica nuova, considerandone il valore all'interno delle proprie attività e processi aziendali. Con la nuova impostazione del Trasporto Pubblico Locale (TPL), Atac ha iniziato a gestire una notevole mole di dati e informazioni, per le quali è stato necessario rivedere e aggiornare, nel tempo e gradualmente, il complessivo impianto dei sistemi informativi e dei servizi informatici dell'azienda.

A ciò si è aggiunta la necessità di una visione aziendale non limitata alla mera gestione di ogni tipologia di mezzi di trasporto, da superficie, a metro e a ferrovie, ma anche alla gestione delle proprie risorse informative.
Queste, da un lato, assicurano agli utenti e ai cittadini livelli adeguati di servizi e di informazioni, per una mobilità sempre più smart e fruibile, e, dall'altro, supportano il personale aziendale nello svolgimento quotidiano dei propri compiti. Il perimetro del sistema di gestione della sicurezza delle informazioni è quindi gradualmente cresciuto nel tempo ed è stato esteso dalla governance delle infrastrutture ICT (certificata nel 2019 secondo la norma ISO/IEC 27001) alle attività di consuntivazione dei servizi sia metro sia superficie, nonché al servizio di rendicontazione degli incassi della sosta e parcheggi, la cui certificazione è in programma.
Questo approccio graduale all'implementazione della norma sui processi aziendali è stato adottato principalmente in considerazione della iniziale necessità di sviluppare delle competenze aziendali in materia, al fine di diffondere una nuova cultura in azienda. A ciò si aggiungeva la necessità di superare gradualmente i limiti tecnologici e di processo dello scenario di partenza. A 3 anni dalla certificazione del perimetro iniziale, oggi Atac SpA risulta tra le prime aziende TPL italiane a ottenere la certificazione ISO/IEC 27001.
Un passo importante nell'evoluzione dell'ambito di applicazione è stato l'inclusione nel 2020 del processo di elaborazione della consuntivazione mensile del servizio di TPL relativo alle metropolitane. Si tratta di uno dei processi fondamentali dell'azienda da cui dipendono i ricavi derivanti dal Contratto di Servizio. A valle della certificazione di questo processo, Atac ha potuto immediatamente sperimentare una riduzione importante del numero di controlli richiesti da Roma Servizi per la Mobilità, l'agenzia comunale che controlla i servizi erogati. Tale riduzione è direttamente attribuibile alla disponibilità e integrità di evidenze derivanti dalla corretta strutturazione dei processi di raccolta e conservazione dei dati relativi al chilometraggio percorso dai mezzi e al numero di corse erogate.
Dal punto di vista dell'adeguamento necessario per la certificazione, il processo è stato fortemente influenzato dai fattori di contesto, in particolare da quelli interni. In tale ambito, sebbene l'azienda avesse già certificato i sistemi di gestione per la qualità e l'ambiente da diversi anni, nella certificazione dell'ISMS, il fattore umano è stato allo stesso tempo sia una leva per spingere verso l'ottenimento della certificazione sia, per certi aspetti, un ostacolo dovuto alla difficoltà di introdurre cambiamenti e novità importanti. In particolare, per quei temi di natura tecnologica e organizzativa, sono state riscontrate delle difficoltà che hanno richiesto un elevato livello di impegno del personale direttamente coinvolto nel processo, al fine di poter superare le verifiche di certificazione. Inoltre, sempre in ambito di fattori interni, alcuni sistemi ereditati dalle aziende prima della fusione (nel 2010 le tre aziende del TPL romano sono state unite nell'attuale Atac SpA) non risultavano in uno stato di controllo tale da rispondere ai requisiti ISO, tali da poter essere inserite in un perimetro di certificazione. Nella pratica, l'impatto di questi fattori si è tradotto in un approfondito lavoro di ritaglio del perimetro di certificazione e nella definizione di piani d'azione necessari per raggiungere la conformità, con un conseguente prolungamento dei tempi per la certificazione.
Anche per il caso di Atac, uno dei requisiti che in fase di adeguamento ha richiesto un maggior sforzo in termini di risorse, sia umane sia tecniche, oltre al contributo di società esterne, è stato la pianificazione del sistema di gestione attraverso l'approccio risk based. In sostanza, l'identificazione, l'analisi e la valutazione dei rischi hanno comportato un forte impegno, soprattutto nel superamento dei limiti culturali preesistenti nell'organizzazione. Sebbene in azienda fosse già presente una funzione di Risk Management, i risultati dell'attività di valutazione dei rischi rispetto ai servizi forniti dall'ICT non rispondevano ai requisiti previsti dalla norma ISO/IEC 27001.

È stato necessario quindi definire un modello di valutazione dei rischi specifico per la sicurezza delle informazioni e per l'ambito di certificazione.
Elemento che ha assunto particolare rilevanza nel caso di Atac è stata la formazione. Infatti Atac, operando da settembre 2017 in regime di concordato preventivo in continuità, non è stata in grado in questi anni di assumere personale specifico per i ruoli associabili alla gestione della sicurezza delle informazioni. In tal senso, sia le risorse della struttura ICT sia alcune di quelle appartenenti alla struttura Sicurezza, Qualità e PMO hanno intrapreso percorsi formativi ad hoc. A titolo esemplificativo, tutte le risorse ICT coinvolte nei principali processi della struttura sono state formate alla norma ITIL e sono stati organizzati appositi corsi sul GDPR ad hoc per amministratori dei sistemi informativi. Sono state avviate, negli ultimi anni, anche iniziative volte a incrementare la consapevolezza rispetto ai rischi cibernetici. I corsi erogati a oggi coinvolgono la dirigenza ed il middle management, ma è in programma un'estensione a una platea di dipendenti più ampia.
Il processo di certificazione ha poi permesso di individuare numerosi spunti di miglioramento. Ad esempio, nel rapporto con i fornitori, si è definita una specifica politica sulla sicurezza degli acquisti ICT volta a definire le misure in materia di sicurezza delle informazioni nei rapporti con i fornitori di beni e servizi, ciò anche al fine di ridurre e limitare il rischio di perdita, danno, furto, compromissione e interruzione della disponibilità, integrità e riservatezza delle informazioni aziendali che vengono gestite e/o utilizzate per mezzo di strumenti informatici.
Certamente Atac è una realtà giovane dal punto di vista della certificazione dell'ISMS, aspetto che rende difficile per l'azienda identificare chiaramente al momento tutte le ricadute derivanti dal processo in corso. Tale processo è stato avviato a partire da un requisito imposto dal Comune attraverso il contratto di servizio per il TPL siglato nel settembre 2015, ma oggi la dirigenza di Atac apprezza le importanti ricadute derivanti dai processi di certificazione, anche se gli effetti organizzativi non sono immediati.

4.3.4 Notartel

In qualità di società del Consiglio Nazionale del Notariato e della Cassa Nazionale e unico erogatore di servizi informatici per i notai italiani, Notartel rappresenta un caso di studio particolare. Il mercato in cui opera non è aperto alla competizione di altri soggetti, e questo naturalmente ha un impatto importante rispetto ai livelli qualitativi dei servizi che Notartel deve erogare. Inoltre molti servizi sono critici per garantire l'erogazione continua e corretta dei servizi di notariato, servizi spesso altrettanto critici per il corretto funzionamento del Paese. Notartel eroga per i notai servizi legati all'uso di certificati digitali come certification authority, servizi di conservazione digitale e posta elettronica certificata. I vincoli AgID, già discussi nel caso Poste Italiane, si applicano anche nel caso di Notartel, che quindi ha la certificazione dell'ISMS come requisito fondamentale per poter erogare i servizi.
Notartel è anche accreditato come soggetto qualificato per l'erogazione di servizi di identità digitale secondo lo standard eIDAS. L'adozione e la certificazione dell'ISMS, inizialmente vissuta da Notartel come un'imposizione, rappresenta oggi un modus operandi che è divenuto parte integrante della cultura aziendale.
In particolare, la certificazione ha imposto l'implementazione di processi che hanno aumentato la consapevolezza del management rispetto ad alcune dinamiche interne all'azienda, con un riflesso indiretto sul miglioramento della qualità dei servizi. Il processo di certificazione è partito nel 2015 con uno scopo limitato ai servizi citati. Negli anni successivi, Notartel ha lavorato per estendere la certificazione a tutti i servizi, anche quelli che non avevano la certificazione come requisito imposto.

La scelta strategica è stata motivata dalla volontà di gestire la sicurezza delle informazioni per i diversi servizi con un approccio omogeneo, anche per favorire l'efficienza.
Uno degli aspetti interessanti emersi dall'analisi del caso Notartel è il costo, in termini di risorse umane, necessarie per il mantenimento delle certificazioni ISO + eIDAS. Le attività di varia natura legate alle certificazioni possono rappresentare un impegno certamente non trascurabile per una realtà di piccole dimensioni. Un altro elemento di interesse della fase di adeguamento di Notartel è rappresentato dal fatto che i consigli distrettuali del notariato sono parzialmente integrati nel perimetro oggetto della certificazione. Queste criticità, tipiche di alcune realtà che lavorano con una presenza locale sul territorio, devono essere tenute in opportuna considerazione nella pianificazione degli adeguamenti necessari per la certificazione.
Particolare attenzione è stata posta da Notartel all'incremento della consapevolezza di tutto il personale relativamente ai rischi legati alla cybersecurity; tutti i programmi di formazione sono curati internamente e coinvolgono l'intero personale con particolare attenzione a quello amministrativo.
Da un punto di vista tecnico, negli ultimi anni Notartel non ha subito particolari incidenti di cybersecurity. A oggi, non è possibile definire se questo dato sia da correlare unicamente a una migliore gestione intervenuta con lo sviluppo formale dell'ISMS, ovvero alla preparazione antecedente alla certificazione.
Certamente, alcune scelte strategiche fatte negli anni, come l'adozione di postazioni virtualizzate per tutti i dipendenti, ha reso più facile l'implementazione di metodologie di contenimento degli incidenti che nei pochi casi riscontrati si sono dimostrate estremamente efficaci. Certamente Notartel pone particolare attenzione all'aspetto dell'innovazione tecnologica, investendo annualmente un budget consistente per l'aggiornamento dei sistemi e per le consulenze in ambito di sicurezza dei sistemi e dei servizi (VA - PT).

4.4 Considerazioni finali

A valle dell'analisi dei casi, è possibile tracciare alcuni **elementi generali legati alla certificazione dell'ISMS**, che si considerano importanti per guidare l'adozione dello standard ISO/IEC 27001 da parte delle organizzazioni che intendono seguire questo percorso.

- Difficilmente le motivazioni che sottendono la decisione di certificare il proprio ISMS rappresenteranno nel tempo l'unico ritorno degli investimenti fatti. Tutte le esperienze raccolte 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.

- La certificazione di un ISMS oggi è un elemento facilitatore per la conformità rispetto ai numerosi regolamenti che, in diversi settori, impongono requisiti legati alla cybersecurity. Praticamente tutti questi regolamenti oggi si basano su schemi che direttamente o indirettamente si rifanno a un approccio basato sulla riduzione del rischio, lo stesso approccio imposto da ISO. Certificare il proprio ISMS in questo senso rende più semplice per l'organizzazione dimostrare per gli aspetti rilevanti il proprio allineamento rispetto alla normativa.

- L'approccio risk based rappresenta, da un lato, uno dei valori aggiunti più importanti acquisiti con l'adozione dell'ISMS, ma anche uno dei punti critici nella fase di adeguamento e successivamente di miglioramento e mantenimento della certificazione. Le attività necessarie sono molteplici, impegnative e spesso richiedono di rivoluzionare il modo di pensare di una organizzazione che si basa su modelli diversi. Il costo, anche in termini di sforzo umano, può essere importante e non necessariamente alla portata dei piccoli operatori o con risorse limitate o che vivono 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 audit indipendenti che permettono di gestire in modo ragionato e coerente criticità, incidenti e futuri adeguamenti.

Da un punto di vista più strettamente legato al processo di certificazione, l'analisi mette in luce delle **strategie generali che risultano efficaci**, dall'esperienza sul campo.

- Nel primo approccio alla certificazione dell'ISMS, è utile procedere per passi incrementali partendo con un ambito di applicazione magari più limitato, ma più facilmente gestibile. Questo "caso pilota" aiuterà l'organizzazione a capire meglio il processo e a individuare le soluzioni più adatte alla propria natura per i problemi che necessariamente emergeranno. Questa esperienza sarà preziosa quando, successivamente, si valuterà l'estensione della certificazione a un ambito più grande.

- Riguardo all'ambito di applicazione del processo di certificazione, se l'organizzazione è grande, diversificata e strutturata geograficamente, è utile valutare correttamente l'ambito finale desiderato per la certificazione. Non necessariamente tutte le funzioni o tutti i rami aziendali dovranno essere certificati. D'altra parte, certificare solo alcuni rami o parti di un gruppo, o specifiche funzioni aziendali, può rappresentare una spinta positiva per allineare metodologicamente anche tutto il resto dell'organizzazione. Questo renderà meno oneroso un eventuale allargamento dell'ambito di certificazione in una fase successiva, abbattendo notevolmente i costi dovuti all'adeguamento.

- Per tutte le organizzazioni che per scelta o imposizione della normativa di settore adottano diversi standard per i quali desiderano certificarsi (es. qualità + ISMS), è importante progettare il sistema di gestione aziendale in modo che al suo interno siano completamente integrati tutti gli aspetti legati alle diverse certificazioni di interesse. Questo permette all'organizzazione di approcciarsi in modo olistico al processo di certificazione, prima acquisendo all'interno gli aspetti culturali, strategici e operativi suggeriti dagli standard e, solo successivamente, affrontando il processo di certificazione per ottenere una valutazione oggettiva di una terza parte accreditata sui propri processi interni. Gli standard per la gestione della sicurezza e i relativi processi di certificazione rappresentano, quindi, 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. È quindi difficile, dopo pochi mesi dalla certificazione, immaginare di avere la consapevolezza sui vantaggi del percorso intrapreso. Questo tipo di investimenti ha un ritorno a lungo termine, che si sostanzia in benefici duraturi che diventano definitivamente parte integrante dell'organizzazione.

5. Attività sul campo

In questo capitolo vengono presentati i risultati di uno studio tecnico su due popolazioni di organizzazioni private e pubbliche italiane, una dotata di certificazione per la sicurezza delle informazioni ISO/IEC 27001 e una dotata di certificazione per la qualità ISO 9001, inteso a valutare la diversa postura di sicurezza delle organizzazioni del campione selezionato, attraverso una campagna di Vulnerability Assessment (non invasiva) dei servizi web esposti al pubblico dalle stesse organizzazioni. Per ogni servizio, sono stati valutati:

1. il corretto utilizzo del protocollo HTTPS;
2. i livelli di aggiornamento e sicurezza dei Content Management System (CMS);
3. il posizionamento dei software utilizzati per tali servizi rispetto alle gravi vulnerabilità note incluse nei database nazionali e internazionali (es. il CVE database [5.16]).

Queste attività, pur non rappresentando una valutazione esaustiva dello stato di sicurezza di un'organizzazione, hanno consentito di effettuare considerazioni preliminari sulla percezione e sul recepimento delle misure basilari di sicurezza informatica introdotte dalle certificazioni. Tali evidenze sono state valutate e discusse, in forma aggregata e anonimizzata, ponendo particolare attenzione alle eventuali diversità tra le organizzazioni certificate ISO/IEC 27001 e quelle prive di certificazione.

5.1 Metodologia di analisi

Questa sezione presenta la metodologia adottata nel presente studio tecnico, una descrizione del campione scelto e le modalità operative di analisi.

5.1.1 Analisi di sicurezza dei servizi Web

La metodologia OSSTMM [5.1] definisce un insieme di processi volti all'analisi di sicurezza di un sistema informatico. Tali processi, declinati nel mondo dei servizi web, permettono di delineare una rigorosa metodologia di verifica della sicurezza.
La metodologia di assessment, integrata con le linee guida di sicurezza definite dall'Open Web Application Security Project (OWASP) [5.25], può essere riassunta nelle seguenti macro-attività:

- **Definizione della superficie di attacco**. La definizione della superficie di attacco permette di specificare il perimetro dell'analisi, identificando tutti i componenti dei servizi web potenzialmente esposti ad attacchi. In questa fase vengono definite anche le modalità di accesso alle informazioni (analisi white-box, grey-box oppure black-box) ed eventuali strumenti automatici o semiautomatici coinvolti nel processo.

- **Individuazione delle tipologie di minaccia**. Questa fase prevede l'individuazione e l'analisi di scenari d'azione costruiti attraverso lo studio del repertorio di minacce conosciute verso i servizi oggetto di analisi.

- **Esecuzione dei controlli**. Per ogni minaccia identificata nella fase precedente, viene eseguita una serie di controlli di sicurezza basati sulla OWASP Application Security Verification Standard (ASVS) [5.2]. Tali controlli vengono tradotti in un elenco tecnico di verifiche di sicurezza, volto a definire in maniera rigorosa la postura di sicurezza del servizio web oggetto di analisi. L'elenco di tali controlli è codificato nella OWASP Web Security Testing Guide (WSTG) [5.3].

- **Identificazione delle vulnerabilità**. In base ai risultati della verifica dei controlli di sicurezza, vengono identificate e analizzate le vulnerabilità che insistono sulla applicazione.

5.1.2 Descrizione del Campione Scelto

Ai fini del presente studio, 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, costituite dalle:

1. organizzazioni provviste della certificazione di sistema di gestione per la sicurezza delle informazioni a norma ISO/IEC 27001;
2. organizzazioni provviste della certificazione di sistema di gestione per la qualità a norma ISO 9001.

Da questi due insiemi sono state escluse quelle organizzazioni che possiedono entrambe le certificazioni per evitare sovrapposizioni tra le due popolazioni. Non sono invece state fatte assunzioni su eventuali altre certificazioni possedute dalle organizzazioni.
Le due popolazioni sono state ulteriormente classificate in sottocategorie tenendo conto dei seguenti criteri:

- dimensione aziendale (micro, piccola, media e grande impresa) [5.4];
- ripartizione geografica (Nord Ovest, Nord Est, Centro, Sud, Isole) [5.5].

Al termine della fase di caratterizzazione delle due popolazioni, sono state estratte 100 organizzazioni, 50 dal primo gruppo e 50 dal secondo, utilizzando la tecnica di "campionamento non probabilistico di convenienza" o "convenience sampling" [5.6].

5.1.3 Descrizione delle modalità di analisi

Le attività di analisi sono state effettuate in modalità black-box, ovvero senza alcuna informazione specifica sui servizi esposti dall'organizzazione (es. eventuale documentazione tecnica). Per fare questo, l'attività tecnica ha ricercato, per ognuna delle organizzazioni oggetto di analisi, l'elenco dei siti web e dei domini disponibili pubblicamente. L'attività di analisi è stata realizzata con il supporto di strumenti automatici di analisi (cmseek [5.7], testssl.sh [5.8], wpscan [5.9], joomscan [5.10]), banche dati di vulnerabilità (NIST National Vulnerability Database [5.11]) e portali di ricerca (Shodan [5.12]). Ogni risultato è stato quindi ispezionato, elaborato e aggregato per la valutazione conclusiva.

5.2 Descrizione dei controlli

In questa sezione vengono dettagliate le 3 classi di controlli oggetto dell'attività tecnica. Tali controlli sono stati estrapolati dalla OWASP Web Security Testing Guide, in linea con una serie di report promossi dal CERT-AgID sui siti della Pubblica Amministrazione [5.13, 5.14, 5.15].

5.2.1 Mappatura delle vulnerabilità tramite fonti OSINT

Il primo set di controlli effettuati riguarda la capacità di valutare le tecnologie, i servizi e le vulnerabilità che possono influire sui servizi web oggetto dell'analisi, tramite l'utilizzo di tecniche di Open Source INTelligence (OSINT), ovvero volte a sfruttare tutte le informazioni pubbliche disponibili e reperibili, come descritto nel set di controlli WSTG-INFO "Information Gathering". Per questo tipo di attività è stato utilizzato come strumento di base Shodan [5.12], un motore di ricerca che raccoglie le informazioni dei dispositivi connessi a Internet. Rispetto a un motore di ricerca ordinaria, che indicizza il contenuto delle pagine web, Shodan cataloga i metadati dei dispositivi, come i banner dei servizi esposti, le porte aperte, le versioni dei software rilevate e altro. Una funzionalità interessante di Shodan è quella di elencare le vulnerabilità note dei software esposti su una specifica macchina. Nel dettaglio, l'attività di mappatura delle vulnerabilità è stata svolta secondo i seguenti passi:

1. individuazione dei domini e degli indirizzi IP delle organizzazioni oggetto di analisi;
2. interrogazione del database di Shodan per individuare un elenco di servizi e porte disponibili pubblicamente;
3. individuazione delle vulnerabilità potenziali associate alle caratteristiche degli indirizzi IP e delle tipologie di servizi disponibili;
4. Individuazione delle tecnologie web utilizzate dai portali dei servizi web tramite lo strumento Wappalyzer [5.22];
5. identificazione di ulteriori vulnerabilità potenziali legate alle tecnologie web utilizzate.

Ognuna delle vulnerabilità è stata classificata secondo il Common Vulnerabilities and Exposures (CVE) [5.16], un elenco di falle nella sicurezza informatica gestito dal MITRE. Nello specifico, ogni vulnerabilità individuata viene associata a un numero identificativo (ID) CVE. Inoltre, per poterne determinare la pericolosità, sono state estrapolate dal database del NIST i corrispettivi Common Vulnerability Scoring System (CVSS) [5.17] che consentono di valutare le caratteristiche di una vulnerabilità e la sua gravità mediante un punteggio numerico.

La versione 3 del CVSS ha introdotto 5 livelli di classificazione di una vulnerabilità basata sul suo score: None (0.0), Low (0.1-3.9), Medium (4.0-6.9), High (7.0-8.9), Critical (9.0-10.0). Tuttavia, è bene ribadire che, trattandosi di un'attività di analisi completamente passiva, le vulnerabilità riscontrate in questa fase sono potenzialmente applicabili ai servizi oggetto di analisi rispetto alle tecnologie e alle configurazioni riscontrate, ma non è possibile farne una validazione attiva, tramite tecniche di penetration testing, che non sono oggetto del presente studio. Seguendo questo approccio, dunque, è possibile che alcune delle vulnerabilità riscontrate dall'attività di information gathering siano non applicabili al servizio web analizzato poiché già risolte/patchate dalle configurazioni esistenti.

5.2.2 Utilizzo sicuro del protocollo HTTPS

Il secondo set di controlli tecnici è volto a individuare eventuali misconfigurazioni o vulnerabilità nell'utilizzo del protocollo HTTPS da parte dei servizi web, come indicato dal controllo WSTG-CRYP-01 "Testing for Weak Transport Layer Security" [5.26]. L'obiettivo del controllo è quello di verificare che il servizio web utilizzi un sistema di comunicazione sicura tramite il protocollo Secure Socket Layer (SSL) e/o Transport Layer Security (TLS) e che tale sistema sia propriamente configurato rispetto agli standard e alle migliori pratiche di sicurezza. Nel dettaglio, il controllo sul corretto utilizzo del protocollo HTTPS consiste nel verificare i seguenti elementi:

- **Utilizzo protocolli SSL/TLS**. Consiste nel verificare la tipologia di protocolli SSL e TLS utilizzati dal servizio web. In particolare, questo tipo di controllo mira a verificare se il sistema sia stato configurato per disabilitare l'utilizzo di protocolli vulnerabili e deprecati come SSLv2, SSLv3 e TLSv1.0.

- **Vulnerabilità legate alla comunicazione SSL**. Questa parte di controllo consiste nel verificare se i protocolli utilizzati dal servizio web sono esposti a una serie di vulnerabilità CVE sulla comunicazione, come la famigerata vulnerabilità Heartbleed [5.18], bug di sicurezza identificato nel 2014 nella libreria OpenSSL e ampliamente utilizzata nel protocollo TLS, che consente a un attaccante di poter accedere ai dati contenuti nel server.

- **Server Cipher Supportati**. Il controllo è volto a verificare il set di cifrari supportati dal server per instaurare una connessione HTTPS rispetto alla lista di oltre 300 disponibili da protocollo [5.19]. In particolare, è necessario verificare che il servizio web non supporti cifrari suscettibili di vulnerabilità o deprecati come indicato nelle configurazioni raccomandate [5.20].

- **Certificati SSL**. In ultimo, il controllo è volto a verificare i certificati esposti dal server, andando a verificare se ciascun certificato sia stato firmato da una trusted authority riconosciuta e se sia in corso di validità.

Raccolti tutti questi dati, il controllo ha provveduto ad associare un valore di rischio a ciascun servizio web. Per il computo del valore di rischio è stato utilizzato il sistema di valutazione proposto nello SSL Server Rating Guide [5.21]. Nel dettaglio, la metodologia consiste nell'assegnare a ogni controllo tecnico una valutazione numerica da 0 a 100. Quindi, ogni categoria viene combinata insieme con il fine di ottenere un grado di valutazione in lettere, secondo la tabella 5.1:

Tabella 5.1 - Grado di Valutazione SSL

Valutazione Numerica	Grado
score >= 80	A
score >= 65	B
score >= 50	C
score >= 35	D
score >= 20	E
score < 20	F

Inoltre, sono stati aggiunti 3 ulteriori gradi:

- A+, per premiare configurazioni particolarmente sicure;
- T ("Trust"), se la verifica non è riuscita a validare il trust di un certificato (e non ci sono altri problemi di sicurezza);
- M ("Mismatch"), quando un server non utilizza effettivamente la crittografia.

L'utilizzo delle nove fasce di valutazione del rischio ha permesso di aggiungere un maggior livello di granularità rispetto alle quattro ("Senza HTTPS", "Grave", "Malconfigurato", "Sicuro") proposte nel report AgID [5.15]. In questo modo, abbiamo due gradi (A e A+) per indicare i siti sicuri, tre gradi (B, C, D) per indicare quelli nella fascia "Malconfigurato", tre gradi (E, F, T) per indicare i siti con valore di rischio "Grave" e infine il grado M per indicare i servizi "Senza HTTP". L'attività di analisi sull'utilizzo sicuro del protocollo HTTPS è stata svolta basandosi sullo strumento di analisi testssl.sh [5.8].

5.2.3 Vulnerabilità nei Content Management System

I Content Management System (CMS) sono sistemi utilizzati spesso per sviluppare servizi e siti web, fornendo un framework modulare e molto versatile per pubblicare contenuti preservando un elevato grado di manutenibilità e configurazione grazie all'inclusione di moduli aggiuntivi, detti plug-in. Tuttavia, negli ultimi anni, tali prodotti sono stati oggetto di numerose vulnerabilità di sicurezza piuttosto gravi, tanto da necessitare una valutazione di sicurezza dedicata nello OWASP Web Security Testing Guide. Per esempio, Joomla [5.27], uno dei CMS più utilizzati, consta più di 400 vulnerabilità CVE individuate negli ultimi 15 anni. In aggiunta, nonostante le patch di sicurezza vengano rilasciate in maniera molto frequente, la moltitudine di tecnologie CMS, possibili configurazioni e differenti plug-in rappresenta de-facto un fattore ostativo per le procedure di aggiornamento, che devono essere effettuate in maniera accurata e periodica, previa la verifica della compatibilità con l'attuale istanza. Questo ostacolo tecnologico, unito a una mancanza di una "cultura dell'aggiornamento" ha portato a una frammentazione sostanziale delle versioni e tipologie di CMS utilizzati dai servizi e dai siti web [5.14].

L'attività di analisi tecnica da noi effettuata ha avuto l'obiettivo di:

- individuare gli eventuali sistemi di CMS (e relative versioni) utilizzati da un sito o servizio web;
- valutare le vulnerabilità legate al CMS e alla versione, utilizzando scanner dedicati come WPscan e Joomscan;

❖ caratterizzare le vulnerabilità CVE estraendo i punteggi CVSS dal database NIST.

È bene notare che non sempre è possibile rilevare correttamente il CMS in uso. Da un lato, non esiste una lista esaustiva e ufficiale di tutti i CMS disponibili e delle versioni più aggiornate. Dall'altro, strumenti di protezione, messi in opera dalle organizzazioni, cercano di rendere i CMS non riconoscibili a fronte di scansioni automatiche eseguite dall'esterno, che un attaccante potrebbe mettere in atto in una fase di ricognizione, per individuare la presenza di eventuali vulnerabilità negli stessi CMS. Come nel caso delle vulnerabilità riscontrate nell'attività di mappatura tramite fonti OSINT, anche quelle individuate sui CMS sono di tipo passivo, ovvero legate alla specifica tecnologia impiegata. Dunque, è possibile che alcune delle vulnerabilità riscontrate dall'attività non siano applicabili al servizio web analizzato poiché già risolte dalle configurazioni esistenti. Per verificare la presenza di tali vulnerabilità, sarebbe necessario effettuare un controllo di tipo attivo (es. penetration testing) che è fuori dagli scopi del presente studio.

5.3 Risultati dell'analisi

5.3.1 Mappatura delle vulnerabilità tramite fonti OSINT

L'attività di analisi sulle vulnerabilità identificate tramite le fonti OSINT ha permesso di individuare 1.207 vulnerabilità CVE sui 100 servizi web oggetto di analisi, di cui 683 (57%) nel campione di organizzazioni certificate ISO 9001 e 524 (43%) nel campione certificato ISO/IEC 27001.

Tabella 5.2 - Ripartizione vulnerabilità tramite fonti OSINT - Organizzazioni certificate ISO 9001

	Critical	High	Medium	Low	
Centro	23	96	116	2	
Isole	27	85	57	0	
Nord Est	7	27	20	0	
Nord Ovest	9	27	43	1	
Sud	21	67	55	0	
TOTALE	87	302	291	3	**683**

Tabella 5.3 - Ripartizione vulnerabilità tramite fonti OSINT - Organizzazioni certificate ISO/IEC 27001

	Critical	High	Medium	Low	
Centro	14	37	52	3	
Isole	19	51	73	1	
Nord Est	0	2	5	0	
Nord Ovest	9	39	35	1	
Sud	31	74	73	5	
TOTALE	73	203	238	10	**524**

Le tabelle 5.2 e 5.3 mostrano, rispettivamente, la ripartizione delle vulnerabilità individuate rispetto alle quattro fasce di rischio (Critical, High, Medium, Low) calcolate utilizzando il corrispettivo punteggio CVSS. In aggiunta, la ripartizione è avvenuta anche su scala geografica (Nord Ovest, Nord Est, Centro, Sud, Isole), evidenziando le zone più soggette a esposizione di rischi cyber legati al numero di vulnerabilità riscontrate. In particolare, è possibile notare come le organizzazioni certificate secondo la norma ISO/IEC 27001 siano – globalmente – meno suscettibili a gravi vulnerabilità di sicurezza, con uno scarto di 14 vulnerabilità Critical e ben 99 vulnerabilità di livello High. Considerando la ripartizione geografica, inoltre, si possono notare delle zone di "eccellenza", come il Nord Est, dove le analisi sulle organizzazioni certificate ISO/IEC 27001 hanno riscontrato solamente 7 potenziali vulnerabilità di sicurezza, di cui 2 High e 5 Medium. Le figure 5.1 e 5.2 mostrano, rispettivamente, la ripartizione delle vulnerabilità individuate all'interno del campione considerato.

Figura 5.1 - Distribuzione Vulnerabilità Potenziali - Organizzazioni certificate ISO 9001

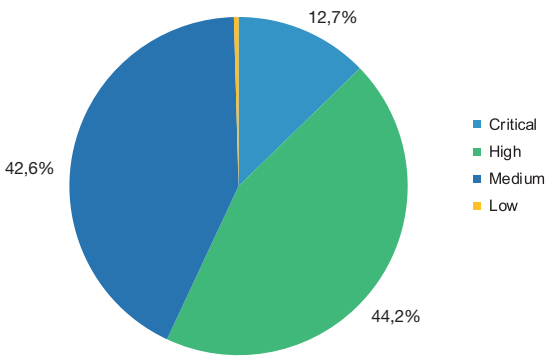
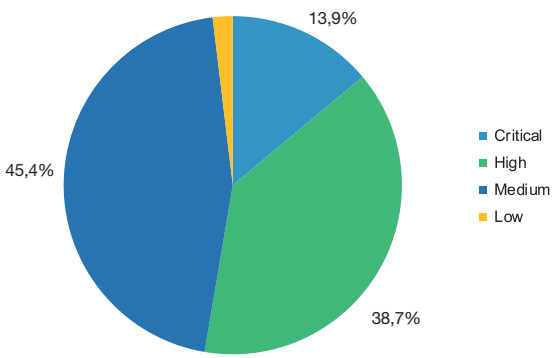


Figura 5.2 - Distribuzione Vulnerabilità Potenziali - Organizzazioni certificate ISO/IEC 27001



La tabella 5.4 dettaglia le dieci maggiori vulnerabilità di livello Critical individuate sui due campioni analizzati.

Tabella 5.4 - Top 10 Vulnerabilità di livello Critical sui due campioni analizzati

Num. Occorrenze	CVE ID	Descrizione Vulnerabilità
19	CVE-2019-9641	La vulnerabilità è causata da una risorsa non inizializzata che potrebbe contenere dati imprevedibili o expired, oppure potrebbe essere inizializzata con valori predefiniti non validi. Questo può influire sulla confidentiality e sulla availability dei dati.
18	CVE-2019-9021	L'over-read del buffer ha un impatto sulla confidentiality dei dati, perché un utente malintenzionato potrebbe essere in grado di aggirare i meccanismi di protezione e leggere i dati riservati.
18	CVE-2019-9020	Attraverso l'inserimento di input non validi, un attaccante può accedere a indirizzi di memoria a cui normalmente non potrebbe accedere, out-of-bound read, e ottenere informazioni riservate.
12	CVE-2020-35489	La vulnerabilità permette a un attaccante di caricare file non consentiti e di eseguire remote code. Influisce negativamente su availability, integrity e confidentiality del dato.
10	CVE-2021-44223	Qualsiasi plug-in personalizzato che utilizza lo stesso slug di un plug-in ospitato su WordPress.org corre un rischio significativo di essere sovrascritto da un aggiornamento di quest'ultimo.
9	CVE-2020-36326	Questa vulnerabilità permette a un attaccante di eseguire una object injection.
7	CVE-2018-1312	La vulnerabilità provoca il fallimento del controllo degli accessi, permettendo a un attaccante di aggirare i meccanismi di autenticazione.
5	CVE-2017-7679	Questa vulnerabilità può portare all'escalation dei privilegi, alla divulgazione di informazioni o al Denial of Service (DoS).
5	CVE-2018-20148	La vulnerabilità permette a un attaccante di performare un PHP object injection attack.
4	CVE-2019-20041	Con l'introduzione di questa vulnerabilità, un utente malintenzionato potrebbe fornire valori imprevisti in input e causare un arresto anomalo del programma o un consumo eccessivo di risorse, come memoria e CPU, potrebbe leggere dati riservati o utilizzare input dannosi per modificare i dati.

Entrando nel merito delle vulnerabilità riscontrate, durante l'attività di analisi sono emersi i seguenti riscontri:

- la vulnerabilità più vecchia riscontrata è CVE-2006-7243, relativa ai servizi web sviluppati in linguaggio PHP con versione antecedente alla 5.3.4, che consentiva di bypassare le restrizioni di accesso; la vulnerabilità, di score Medium, è stata riscontrata su una azienda appartenente al campione delle organizzazioni certificate a norma ISO 9001;

- le organizzazioni sono risultate suscettibili a 16 vulnerabilità CVE del 2022 di severità da Medium a Critical, che interessano 21 diversi servizi web esposti al pubblico;

- la Top 10 delle vulnerabilità di livello Critical, dettagliata in tabella 5.4, mostra come le vulnerabilità CVE critiche che affliggono più servizi web sono dovute a vulnerabilità riscontrate sulle tecnologie PHP, Apache httpd e il CMS Wordpress.

5.3.2 Utilizzo sicuro del protocollo HTTPS

L'attività di analisi sull'utilizzo del protocollo HTTPS ha riportato i risultati visibili in figura 5.3 (relativi alle organizzazioni certificate ISO/IEC 27001) e in figura 5.5 (relativi alle organizzazioni certificate ISO 9001). In particolare, **le organizzazioni certificate secondo la norma ISO/IEC 27001** hanno collezionato 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 (score maggiore o uguale a 65 su cento), superando pienamente la sufficienza.

Figura 5.3 - Valutazione SSL del campione di organizzazioni certificate ISO/IEC 27001

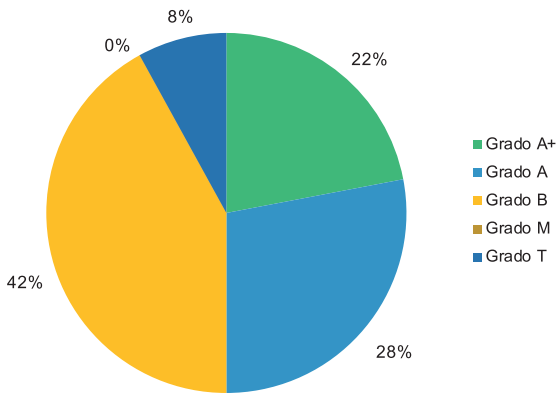
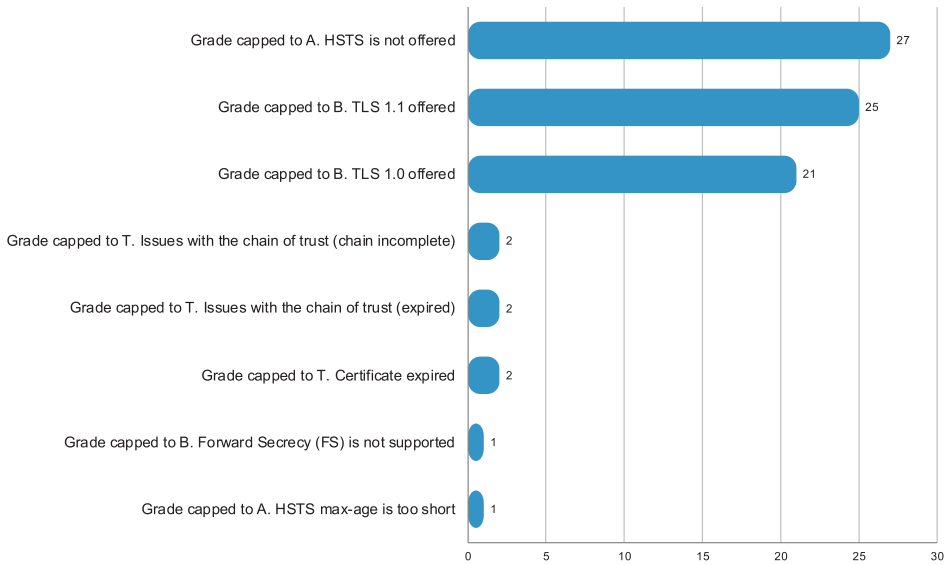


Figura 5.4 - Principali motivazioni della valutazione SSL delle organizzazioni certificate ISO/IEC 27001



Visionando le ragioni che hanno portato a gradi più bassi (figura 5.4) si evidenzia come, nella maggior parte dei casi, il punteggio più basso sia dovuto al supporto di configurazioni SSL a protocolli di tipo legacy come TLS 1.1 e TLS 1.0 (protocolli vulnerabili a una serie di attacchi e deprecati dalle raccomandazioni AgID [5.23]), oppure per l'assenza della configurazione di Strict Transport Security (HSTS) [5.24], che impedisce a una comunicazione di essere rediretta su un protocollo non sicuro (HTTP). In ultimo, l'8% (pari a 4 servizi web) ha ottenuto come valutazione T, a causa di problemi di attendibilità del certificato.
Per quanto riguarda, invece, le organizzazioni certificate secondo la norma ISO 9001 (figura 5.5), 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. Le motivazioni che portano all'ottenimento del grado B sono, come visibile in figura 5.6, analoghe a quanto riportato per le organizzazioni ISO/IEC 27001. Nel caso delle organizzazioni certificate ISO 9001 troviamo però un 4% di servizi web che hanno ottenuto il grado M, non offrendo una connessione di tipo HTTPS per accedere ai loro servizi. Questa situazione rappresenta una seria minaccia alla confidenzialità e integrità dei dati condivisi con il servizio web, specie in uno dei domini analizzati che risulta essere uno shop online. Il 9% dei servizi ha ottenuto grado T, dovuto a un errore di validazione dei certificati esposti dal servizio. Infine, rispetto al report AgID [5.15], è possibile notare come sia le organizzazioni ISO/IEC 27001 sia quelle ISO 9001 abbiano – globalmente – una migliore postura di sicurezza rispetto alle controparti della PA, che possiedono servizi web classificati come "Sicuri" (gradi A, A+) nel solo 22% dei casi.

Figura 5.5 - Valutazione SSL del campione di organizzazioni certificate ISO 9001

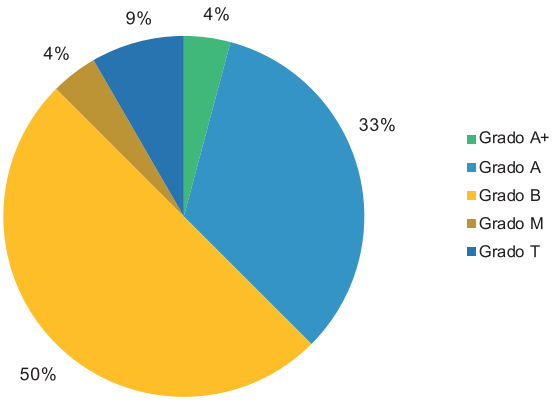
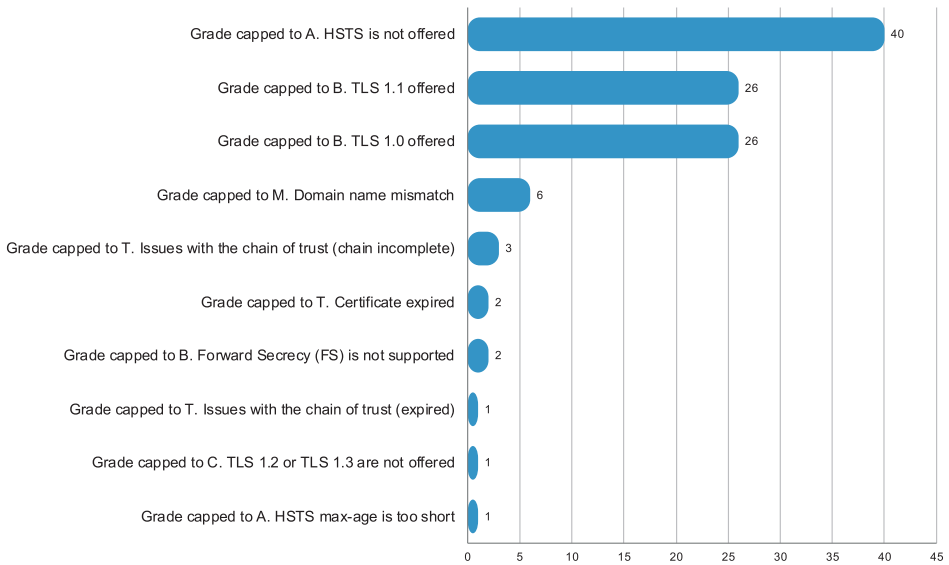


Figura 5.6 - Principali motivazioni della valutazione SSL delle organizzazioni certificate ISO 9001



5.3.3 Vulnerabilità nei Content Management System

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 come riportato in tabella 5.5. La piattaforma di CMS più utilizzata risulta WordPress, con 51 installazioni.

Tabella 5.5 - Tecnologie di Content Management Systems rilevate durante l'analisi

TIPI di CMS	Numero Installazioni
WordPress	51
Joomla	6
Drupal	2
DNN Platform	1
Microsoft Sharepoint	1
OpenCms	1
Concrete5 CMS	1
WIX Website Builder	1
TOTALE	64

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.
L'analisi – riassunta in figura 5.7 e in figura 5.8 – ha riscontrato che **il 24% delle organizzazioni certificate ISO/IEC 27001** risulta avere una **versione aggiornata del proprio CMS**, a differenza della controparte certificata ISO 9001 che si attesta al 18%. Globalmente, più del 20% delle istanze invece ha versioni obsolete e potenzialmente vulnerabili. In alcuni casi, non è stato possibile rilevare automaticamente la versione del CMS (22% nelle organizzazioni ISO/IEC 27001, 14% nelle organizzazioni ISO 9001). Questo risultato può essere dovuto sia a plug-in di sicurezza installati sul servizio web, che mirano a nascondere la versione del CMS per evitare che strumenti di attacco automatici possano utilizzare exploit conosciuti in base alla versione riscontrata, sia all'incapacità – da parte degli strumenti dello stato dell'arte – di riuscire a identificare la versione in uso.

Durante l'attività di analisi sono emerse le seguenti considerazioni:

- la versione più obsoleta di CMS riscontrata è Joomla versione 1.5 di settembre 2012, utilizzata da un sito web di una organizzazione certificata ISO 9001. Tale versione ha più di 1.000 diversi CVE applicabili;

- la tecnologia più utilizzata (WordPress) ha al suo attivo 4.325 CVE registrati; questo evidenzia come l'utilizzo di tale strumento debba essere monitorato con estrema attenzione, andando ad aggiornare con frequenza le versioni e i plug-in utilizzati.

Figura 5.7 - Analisi Distribuzione utilizzo CMS nel dataset delle organizzazioni certificate ISO/IEC 27001

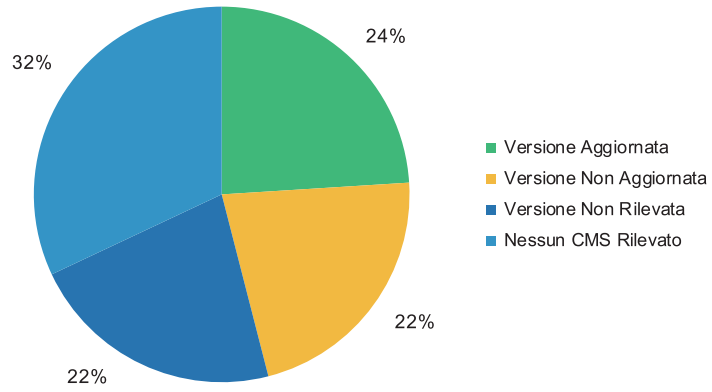
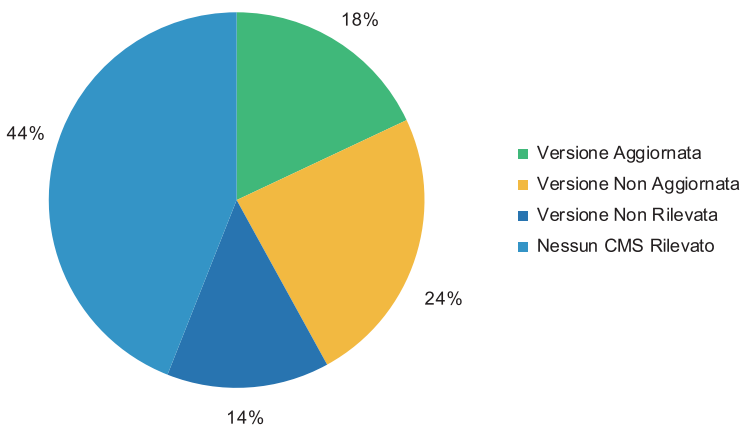


Figura 5.8 - Analisi Distribuzione utilizzo CMS nel dataset delle organizzazioni certificate ISO 9001



5.4 Conclusioni

L'analisi condotta – pur non rappresentando una valutazione esaustiva dello stato di sicurezza di un'organizzazione – ha permesso di delineare come le organizzazioni certificate secondo la norma ISO/IEC 27001 siano globalmente meno suscettibili a gravi vulnerabilità di sicurezza rispetto alla controparte delle organizzazioni certificate a norma ISO 9001.
In particolare, le prime hanno impostato un utilizzo dei protocolli di comunicazione sicura SSL direzionato verso configurazioni di massima sicurezza (50% delle aziende con valutazioni A o A+) e hanno mostrato una leggera prevalenza nell'aggiornare le proprie tecnologie di CMS rispetto alle organizzazioni certificate ISO 9001, mitigando quindi le innumerevoli vulnerabilità di sicurezza legate a questi strumenti. In generale, le organizzazioni con certificazione ISO/IEC 27001 evidenziano una postura di sicurezza migliore rispetto a quelle certificate ISO 9001.

6. Prospettive dei servizi accreditati di cybersecurity

Come illustrato nel capitolo 3, i servizi di valutazione della conformità (certificazioni, ispezioni, verifiche e validazioni, prove e tarature, ecc.) svolti dagli organismi e dai laboratori accreditati, assicurando il rispetto di norme e standard riconosciuti a livello nazionale e internazionale, offrono garanzie sulla qualità e sulla sicurezza dei prodotti e dei servizi acquistati. **Il beneficio apportato dai servizi accreditati è importante in una varietà di ambiti, ma diventa cruciale in un ambito sensibile quale quello della cybersecurity**. Essi offrono, infatti, garanzie circa il rispetto di requisiti di sicurezza fondamentali quali la tutela della privacy e la protezione dell'erogazione dei servizi essenziali dalla minaccia cyber. 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 dalla minaccia cibernetica, quali ad esempio la Strategia Nazionale di Cybersicurezza, pubblicata da ACN, e il Cybersecurity Act [2.1]. Nel presente capitolo proviamo a ipotizzare possibili sviluppi dei servizi accreditati di cybersecurity negli anni a venire alla luce di dette iniziative.

6.1 Il Cybersecurity Act

Come descritto in sezione 2.1, il Regolamento UE 2019/881 (Cybersecurity Act) mira a creare un quadro europeo per la certificazione della sicurezza informatica di prodotti ICT e servizi digitali con l'obiettivo di:

1. creare un mercato unico della sicurezza cibernetica in termini di prodotti, servizi e processi ICT;
2. facilitare lo scambio degli stessi all'interno dell'Unione europea;
3. accrescere la fiducia dei consumatori nelle tecnologie digitali.

A tal fine introduce un quadro complessivo di regole che disciplinano gli schemi europei di certificazione della sicurezza informatica; tuttavia non definisce schemi di certificazione direttamente operativi, ma crea un framework di base su cui istituire schemi europei per la certificazione. La creazione di questi schemi di certificazione, da predisporsi per specifiche categorie di prodotti e servizi, è demandata all'Agenzia Europea per la Cybersecurity (ENISA).
I certificati rilasciati secondo tali schemi saranno validi e riconosciuti in tutti gli Stati membri.

Gli schemi europei di certificazione andranno gradualmente a rimpiazzare gli omologhi schemi di certificazione nazionali, ove esistenti, che rimarranno validi fino alla loro scadenza naturale. Le aziende interessate potranno presentare domanda di certificazione dei propri prodotti o servizi, a seconda di quanto stabilito da ENISA, o all'Agenzia Nazionale per la Cybersecurity dei pertinenti Stati membri dell'Unione, o direttamente a dei laboratori appositamente accreditati. Ciò, salvo che lo schema di certificazione in questione non consenta alle aziende di procedere a una autovalutazione di conformità (solo per prodotti e servizi a basso rischio). L'utilizzo della certificazione rimarrà tuttavia volontario, a meno che la certificazione venga espressamente richiesta da provvedimenti cogenti, per determinate categorie di prodotti o servizi, sulla base di specifiche norme di settore.
I vantaggi portati dalla creazione di un mercato europeo della certificazione della sicurezza informatica di prodotti ICT e servizi digitali sono molteplici e importanti. In primo luogo, i certificati rilasciati secondo gli schemi di certificazione europei saranno validi e riconosciuti in tutti gli Stati membri.

6.2 La Strategia Nazionale di Cybersicurezza

La Strategia Nazionale di Cybersicurezza è posta in continuità con i provvedimenti normativi di recepimento della Direttiva EU 2016/1148, nota come NIS (Network and Information Security) 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 CVCN e dovranno seguire le prescrizioni di sicurezza fornite dall'ACN. Quindi, a oggi, si ha uno scenario nel quale un numero non definito, ma verosimilmente di diverse centinaia di operatori, è già stato inserito nel perimetro nazionale.
Le attività dell'Agenzia saranno principalmente riferite al monitoraggio degli approvvigionamenti di beni ICT. Ciò significa che il lavoro numericamente più significativo sarà svolto in relazione alle certificazioni di prodotto (dispositivi di rete e di sicurezza delle reti e, almeno in parte, anche di dispositivi di sicurezza per il controllo di reti industriali).
Questo servizio si realizzerà attraverso un processo di accreditamento che comunque ricadrà sotto le previsioni del Regolamento CE 765/2008, tramite la collaborazione operativa tra l'ACN, Accredia e i laboratori accreditati da Accredia stessa.
Oltre le certificazioni di prodotto, di particolare rilevanza è l'area delle certificazioni degli ISMS, ma anche dell'erogazione dei servizi ICT di tipo fiduciario. Senza questa componente sistemica, le sole certificazioni di prodotto, come quelle sopra descritte, rischiano di non avere l'effetto desiderato. Basti pensare all'impatto del solo fattore umano (ovvero errori da parte delle persone, ad esempio nell'utilizzo operativo quotidiano dei dispositivi ICT) che viene gestito proprio a livello sistemico e non a livello di prodotto.
Per comprendere l'importanza dell'aspetto sistemico-organizzativo, si pensi ad esempio a un dispositivo ICT che, per quanto certificato, debba essere installato, manutenuto, utilizzato da persone che hanno maggiore o minore consapevolezza nell'ambito di regole e policy di sicurezza, proprio quelle che permettano di garantirne il corretto impiego.
Di fatto, gli organismi accreditati da Accredia per i sistemi di gestione svolgono il monitoraggio (certificazione iniziale, sorveglianze e rinnovi) di circa 4.200 aziende a cui vanno sommate oltre 350 aziende per lo schema ITSMS).

Va ricordato che alcuni accreditamenti di Accredia, che autorizzano gli organismi di certificazione a operare nell'ambito regolamentato *trusted*, cioè fiduciario, sono relativi alle certificazioni di servizio (area prodotto) e coinvolgono la vigilanza dell'AgID. Si tratta di servizi quali SPID e quelli previsti dal Regolamento eIDAS. In un prossimo futuro riguarderanno la gestione della filiera di accreditamento-certificazione in ambito GDPR. Torniamo ai numeri: 4.200 organizzazioni certificate da 20 organismi di certificazione detentori di circa 30 accreditamenti, che, unite ai 5 laboratori e ai *Trust Service Providers* in ambito SPID ed eIDAS, assommano a circa 4.300 soggetti, che rappresentano circa un millesimo del tessuto produttivo dell'intero Paese. La creazione del *know-how* dei professionisti impiegati non è un processo breve né semplice. Ad esempio, i professionisti in possesso di certificazione professionale per svolgere gli audit nell'ambito della sicurezza delle informazioni non superano i 40 in tutto il Paese. Tale limitazione risiede nel fatto che la crescita in un comparto – tanto più se di nicchia, come quello della sicurezza delle informazioni – avviene per piccoli incrementi, che garantiscano un equilibrio tra costi e margini. Questi ultimi, peraltro, sono sempre più risicati a causa delle dinamiche complessive della contingenza economica e del mercato. Una novità interessante, che richiede un'attenta riflessione, verrà introdotta dalla futura Direttiva EU, denominata NIS2, che potrebbe allargare il perimetro delle organizzazioni sotto il monitoraggio dell'ACN a diverse migliaia di unità, potenzialmente più di 10.000. Siamo quindi di fronte a una sfida molto complessa, considerando che, per arrivare al traguardo di 4.200 organizzazioni certificate sotto accreditamento per la norma ISO/IEC 27001, sono serviti 20 anni. Il perimetro di sicurezza allargato indotto dalla NIS2 potrebbe pertanto porci di fronte a oggettive difficoltà in termini della capacità di azione nel breve-medio periodo.
In conclusione, possiamo affermare che il mercato in ambito sicurezza delle informazioni e cybersecurity è oggi presidiato dai servizi di auditing e certificazione riconducibili alla catena operativa costituita dagli organismi di certificazione accreditati da Accredia (di tipo volontario e quasi volontario), mentre nel perimetro di sicurezza nazionale opera invece. Un dialogo e una stretta collaborazione tra i 2 Enti non solo è indispensabile, ma è già attiva e consolidata da rapporti di reciproca fiducia e condivisione di valori sostanziali di utilità per il Sistema Paese.

6.2.1 La Strategia Nazionale di Cybersicurezza: un focus sull'attività di formazione

Come evidenziato nei paragrafi precedenti, un elemento centrale della Strategia Nazionale di Cybersicurezza è rappresentato dalla formazione e dalla promozione della cultura sulla sicurezza cibernetica, a cui sono dedicate dodici missioni. L'obiettivo è promuovere una conoscenza diffusa sui rischi connessi all'utilizzo di strumenti digitali e diffondere specifiche competenze in materia di cybersecurity, al fine di realizzare una società più matura e preparata.
In primo luogo, si prevede dunque un rafforzamento dei percorsi formativi, a partire dalle scuole elementari fino ai dottorati di ricerca (misura #59), con un focus specifico sugli Istituti Tecnici Superiori (ITS) (misura #60). In secondo luogo, si ipotizzano percorsi di apprendimento, per tutti i cittadini e le cittadine, che consentano, al termine delle lezioni, di auto-testare le competenze e le sensibilità acquisite e di ottenere un attestato (misura #62). In terzo luogo, si intende realizzare misure volte a migliorare l'inserimento lavorativo dei giovani con competenze sulla cybersecurity, sostenendo altresì le start up che si occupano di cybersecurity (misure #63, #64 #65, #66). In quarto e ultimo luogo, ci si concentra sulla formazione del personale pubblico (in particolare del corpo diplomatico) e privato, anche attraverso appositi corsi di aggiornamento (misure #67, #68, #69, #70).

Al fine di garantire l'efficacia dei percorsi formativi, si prevede 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 (misura #61). L'ACN dovrà mantenere una lista dei percorsi di formazione, approvati dalla stessa Agenzia, al termine dei quali il discente conseguirà, oltre al titolo di studio/professionale, la relativa certificazione. Si noti come le misure proposte si basino su forme di cooperazione tra pubblico e privato. A livello normativo, sia il DL 82/2021 (art. 7) sia il D.Lgs. 123/2022 (art. 9) hanno già previsto che le attività di formazione e ricerca dell'ACN potranno essere realizzate con il supporto di Enti pubblici (Università, centri di ricerca) e privati (es. laboratori specializzati, Enti di formazione accreditati) e con il supporto di ENISA ai sensi del Regolamento 881/2019. In una materia in costante evoluzione come quella della sicurezza cibernetica, risulta infatti fondamentale mettere a sistema tutto il know-how presente a livello nazionale ed europeo. In questa prospettiva, sistemi di accreditamento di professionisti, laboratori e organismi di valutazione della conformità accreditati potranno facilitare l'ACN e la Pubblica Amministrazione nella scelta di partner qualificati e conformi alle normative di riferimento. Lo scambio di informazioni e di buone pratiche, come ribadito nella Strategia nazionale, nella normativa nazionale e nei Regolamenti europei, permetterà di sviluppare un network europeo delle cybersecurity, sempre più resiliente e capace di fronteggiare le sfide future.

6.3 Prospettive dei servizi accreditati di cybersecurity

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. Ad esempio, i tempi e i costi associati alla certificazione di prodotti e servizi spesso non sono compatibili con i vincoli finanziari e/o di time-to-market a cui sono soggette le aziende produttrici. Ad esempio, non tutti i prodotti e i servizi richiedono il livello di sicurezza (*assurance level*) offerto dalla norma ISO/IEC 15408 Common Criteria, né le relative aziende produttrici (si pensi a una PMI) sono in grado di sostenere i relativi costi. Per cogliere appieno le opportunità offerte dalla crescente attenzione sui servizi accreditati di cybersecurity, posta dalle succitate iniziative nazionali e comunitarie, è pertanto fondamentale che gli schemi di certificazione di cybersecurity possano evolvere nelle direzioni richieste dal mercato.

6.3.1 Schemi di certificazione "leggera" o "di base"

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.
Alcune nazioni hanno già effettuato alcuni passi in questa direzione, mediante la messa a punto di metodologie di valutazione basati su approcci semplificati ai Common Criteria [3.1]:

- LINCE [6.1] sviluppata dal Centro *Criptológico Nacional* (CCN) spagnolo, è caratterizzato da un limitato ricorso alla valutazione della documentazione a favore di una focalizzazione su black-

box *vulnerability assessment e penetration testing*, consentendo di identificare le vulnerabilità più severe con un costo contenuto.

- CSPN [6.2] proposta dall'*Agence nationale de la sécurité des systèmes d'information* (ANSSI) francese, è stata introdotta come alternativa ai Common Criteria per consentire la valutazione della resistenza di un prodotto a un attacco di livello moderato.

- BSZ [6.3] sviluppato dal *Bundesamt für Sicherheit in der Informationstechnik* (BSI) - Federal Office for Information Security tedesco, fornisce una certificazione di sicurezza "accelerata" che costituisce un compromesso tra il livello di assurance offerto e il tempo necessario per condurre la valutazione, ottenuta combinando il testing di conformità e il penetration testing.

- BSPA [6.4] gestito dall'*Algemene Inlichtingenen Veiligheidsdienst* (AIVD) - General Intelligence and Security Service olandese, è ispirato al CSPN francese ed è focalizzato su prodotti hardware e software di cybersecurity per ambiti sensibili, ma non classificati. Ai fini della valutazione, sono necessari solo una versione installata e funzionante del prodotto e la relativa documentazione.

Il lavoro richiesto per l'applicazione di tali metodologie si attesta mediamente sulle 25 giornate lavorative, che possono essere incrementate qualora siano necessari approfondimenti specifici (es. l'analisi delle primitive crittografiche).

6.3.2 Integrazione della certificazione di cybersecurity nel processo di sviluppo

È ben noto che nell'industria del software si sia recentemente imposto il paradigma DevOps, ovvero di una metodologia basata su una combinazione di pratiche e strumenti che consentono alle organizzazioni di rendere disponibili nuove applicazioni e servizi o far evolvere applicazioni e servizi esistenti a una velocità impensabile solo pochi anni fa. Il DevOps combina le fasi di sviluppo (*Development*) e di messa in operazione (*Operations*) del software assicurando così che le nuove funzionalità introdotte in fase di sviluppo vengano messe in operazione in tempi rapidissimi, garantendo, nel contempo, un alto livello di qualità.
Questo risultato viene ottenuto evitando di compartimentare i team di sviluppo e di messa in operazione fino ad arrivare, in alcuni casi, a una vera e propria fusione in un singolo team, i cui membri lavorano all'intero ciclo di sviluppo dell'applicazione (sviluppo, testing, installazione e esecuzione). In alcuni casi anche il personale dedicato alla cybersecurity viene integrato nelle fasi di sviluppo e di messa in operazione e ciò contribuisce a propagare la consapevolezza delle problematiche di sicurezza in tutto il ciclo di vita dell'applicazione. In questi casi il paradigma DevOps viene promosso a *DevSecOps*.
Il modello DevSecOps apre degli scenari molto 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 consente 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. Si tratta di uno sviluppo che potrà contribuire a rendere ancora più efficienti, sia dal punto di vista dei tempi sia dei costi, gli schemi di certificazione di cybersecurity "leggeri" introdotti nella sezione 6.4.1.

6.3.4 Cyber-Range per le certificazioni di cybersecurity

I *Cyber-Range* (Poligoni Virtuali, in italiano) sono piattaforme informatiche che, grazie alle tecnologie della virtualizzazione, supportano la simulazione di attacchi cyber in scenari ICT di elevato realismo. I Cyber-Range sono stati inizialmente introdotti in ambito militare per condurre esercitazioni di *Cyber Defence* e verificare così la capacità di risposta delle unità militari preposte alla difesa delle infrastrutture strategiche dei rispettivi Paesi. *Locked Shields*[26], la più importante esercitazione di Cyber Defence al mondo, è condotta utilizzando il Cyber-Range del *Cooperative Cyber Defence Centre of Excellence* (CCDCOE) della NATO a Tallinn (Estonia). E' oggi ampiamente riconosciuto che il potenziale offerto dai Cyber-Range trascende l'ambito militare, in cui sono nati, e che la possibilità di verificare la capacità di risposta non solo del personale, ma anche degli apparati e delle procedure preposte alla difesa e alla resilienza delle infrastrutture dalla minaccia cyber, sta diventando un imperativo in molti ambiti.
I Cyber-Range offrono altresì la possibilità di verificare la resilienza dei servizi erogati dalle aziende di fronte a minacce sofisticate e pervasive rappresentate da ransomware di ultima generazione. I Cyber-Range, supportando l'esecuzione di attacchi sofisticati e su larga scala, ma nel contempo in sicurezza (ovvero senza rischi per i sistemi e i servizi in esercizio) offrono 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. Tali schemi potranno essere basati sulla verifica dell'efficacia delle misure di sicurezza e della resilienza dei sistemi in condizioni molto simili a quelle di esercizio e con sollecitazioni corrispondenti ad attacchi sofisticati e di larga scala, con un bacino d'utenza molto ampio, che include il settore finanziario, delle telecomunicazioni, energetico e dei trasporti.

6.4 Certificazioni di cybersecurity per le PMI

Sia gli schemi di certificazione sia i framework di cybersecurity sono spesso realizzati avendo come obiettivo primario le grandi organizzazioni. Ne consegue che la complessità e i costi associati ai servizi accreditati di cybersecurity sono spesso fuori dalla portata delle aziende meno strutturate da un punto organizzativo e con limitate capacità di spesa, quali ad esempio le PMI. Questo è un problema acuto, specialmente per il nostro Paese, la cui economia è caratterizzata da una presenza molto consistente di PMI. Secondo la European Cyber Security Organization (ECSO) [6.5] la quasi totalità (98%) delle 60.000 aziende che operano nel mercato europeo della cybersecurity sono PMI o *Start-up*.
Nell'ambito delle attività condotte dal progetto SPARTA[3.1], è stata realizzata una indagine dei servizi (accreditati e non) di cybersecurity accessibili alle PMI in Europa. La tabella 6.1 ne riporta una versione adattata ed estesa, concepita per gli obiettivi del presente rapporto.
Come si può vedere, pur esistendo diverse soluzioni offerte nei vari paesi europei, manca uno schema di certificazione unificato dedicato alle PMI. Tuttavia, come evidenziato nella sezione 6.1, il Cybersecurity Act potrà offrire alle PMI gli strumenti di certificazioni adeguati per affrontare le sfide del mercato e superare i limiti degli schemi di certificazione attualmente disponibili.

[26] *https://ccdcoe.org/exercises/locked-shields/*

Tabella 6.1 - Comparazione dei principali schemi di certificazione e framework di cybersecurity disponibili per le PMI - Adattato ed esteso da SPARTA (EU H2020 Project)

	Tipo	Paese	Website	Organizzazione	PMI	Controlli	Strumenti
Cyberessentials	Attestato	Regno Unito	https//www.cyberessentials.org	National Cyber Security Centre	Sì	Cinque controlli principali: - firewall/gateway - programmazione sicura - controllo degli accessi - protezione dal malware - gestione delle patch	Autovalutazione online
Certificazione ANSSI	Attestato	Francia	https://www.ssi.gouv.fr/en/certification/common-criteria-certification/	ANSSI	Sì		
BSI	Raccomandazione	Germania	https://www.bsi.bund.de/EN/Topics/Certification/certification_node.html	BSI	Sì	Basata sulla famiglia ISO 2700x	Catalogo dellle "Minacce Elementari"
VDS	Certificazione (privata)	Germania	https://vds.de/en/vds-quick-check	VdS	Sì	Quattro aree: - organizzazione - tecnologia - prevenzione - gestione (39 controlli veloci)	Autovalutazione online
Framework Nazionale di Cybersecurity	Framework	Italia	https://www.cybersecurityframework.it/	Lab. Naz. di Cybersecurity del CINI e CIS Sapienza	Include linee guida e contestualizzazione per PMI	Basato sul CSF del NIST 11 linee guita operazionali	Diversi strumenti a supporto dell'adozione e diffusione del framework
ISO27001	Standard	Internazionale	https://www.iso.org/iso-iec-27001-information-security.html	ISO	No	130 controlli di sicurezza individuali raggruppati in 11 area chiave	Numerosi strumenti disponibili
Cybersecurity Framework	Framework	USA/Internazionale	https://www.nist.gov/cyberframework	NIST	Viene fornito adattamento	Cinque funzioni: - identifica - proteggi - rileva - rispondi - recupera	CSF Reference Tool
ISSA 5173	Standard	Regno Unito	https://issa.org.pl/63-issa-uk-draft-standard-on-information-security-for-smes/file	ISSA	Sì	circa 10 categorie	
Controlli CIS	Buona pratica	USA/Internazionale	https://www.sans.org/blog/cis-controls-v8/	Center of Internet Security	Sì	20 controlli	Numerosi strumenti automatizzano i controlli
Cybersecurity Labelling Scheme (CLS)	Label	Singapore	https://www.csa.gov.sg/Programmes/certification-and-labelling-schemes/cybersecurity-labelling-scheme/about-cls	Cyber Security Agency of Singapore	SI	Circoscritti a dispositivi connessi in rete (WIFi routers, IoT) Analoghi ai controlli per le web app proposti da OWASP: - dichiarazioni di conformità da parte dei produttori - analisi e test da parte di laboratori indipendenti	Gestito dall'Agenzia nazionale attraverso laboratori di valutazione
Cyber Essential / Cyber Trust	Certification for enteprises	Singapore	https://www.csa.gov.sg/Programmes/sgcybersafe/cybersecurity-certification-for-enterprises/cybersecurity-certification-scheme-for-enterprises	Cyber Security Agency of Singapore	SI	22 controlli per Cyber Trust Analisi meno approfondita per Cyber Essentials	Centri di certificazione accreditati da Agenzia Nazionale Cyber Security

Tabella 6.1 - Comparazione dei principali schemi di certificazione e framework di cybersecurity disponibili per le PMI - Adattato ed esteso da SPARTA (EU H2020 Project)

	Tipo	Paese	Website	Organizzazione	Schema	Livello (maturità o progresso)	Anno di creazione
Cyberessentials	Attestato	Regno Unito	https//www.cyberessentials.org	National Cyber Security Centre	Schema di accreditamento del governo del Regno Unito	due livelli	2013
Certificazione ANSSI	Attestato	Francia	https://www.ssi.gouv.fr/en/certification/common-criteria-certification/	ANSSI	Basato sui Common Criteria	due livelli: "primo livello" e Common Criteria con diversi EAL	2015
BSI	Raccomandazione	Germania	https://www.bsi.bund.de/EN/Topics/Certification/certification_node.html	BSI			2008
VDS	Certificazione (privata)	Germania	https://vds.de/en/vds-quick-check	VdS	Organismo di certificazione che approva il fornitori di servizio per un periodo di tempo limitato	quattro livelli	2017
Framework Nazionale di Cybersecurity	Framework	Italia	https://www.cybersecurityframework.it/	Lab. Naz. di Cybersecurity del CINI e CIS Sapienza		quattro livelli	2015
ISO27001	Standard	Internazionale	https://www.iso.org/iso-iec-27001-information-security.html	ISO			2013
Cybersecurity Framework	Framework	USA/Internazionale	https://www.nist.gov/cyberframework	NIST		quattro livelli	2014
ISSA 5173	Standard	Regno Unito	https://issa.org.pl/63-issa-uk-draft-standard-on-information-security-for-smes/file	ISSA		tre livelli di maturità	2011
Controlli CIS	Buona pratica	USA/Internazionale	https://www.sans.org/blog/cis-controls-v8/	Center of Internet Security			2008
Cybersecurity Labelling Scheme (CLS)	Label	Singapore	https://www.csa.gov.sg/Programmes/certification-and-labelling-schemes/cybersecurity-labelling-scheme/about-cls	Cyber Security Agency of Singapore		quattro livelli	2020
Cyber Essential / Cyber Trust	Certification for enteprises	Singapore	https://www.csa.gov.sg/Programmes/sgcybersafe/cybersecurity-certification-for-enterprises/cybersecurity-certification-scheme-for-enterprises	Cyber Security Agency of Singapore	Orientato a portare aziende verso ISO/IEC 27001	cinque livelli per Cyber Trust	2022

7. Considerazioni finali

Il dominio della cybersecurity ha, nella sua variegata composizione, un aspetto concettuale peculiare. Adottare delle misure adeguate[27] di cybersecurity significa ottenere un sufficiente grado di garanzia che sistemi, processi, prodotti, servizi, organizzazioni, in riferimento a tutto ciò che è legato all'IT e quindi al Cyberspazio[28], funzionino correttamente nello svolgimento della propria missione, anche nell'ipotesi che essi operino in ambiente ostile. A partire da questo assunto, si potrebbe concludere che tale garanzia sia molto impegnativa e difficile da raggiungere, nella misura in cui l'avversario ha il vantaggio della sorpresa e della scelta del veicolo di attacco. Dal punto di vista disciplinare, l'apparente paradosso sopra esposto, si traduce nel prendere atto del fatto che, per raggiungere un livello di garanzia "adeguato" dal punto di vista pratico, non è certamente sufficiente stabilire adeguate politiche di sicurezza e definire e implementare i relativi meccanismi di sicurezza capaci di attuare le politiche. È, infatti, fondamentale progettare politiche e meccanismi in funzione del tipo di minaccia considerato (il cosiddetto *threat model*) e, soprattutto, accertarsi del fatto che tale modello di minaccia sia realistico e che vi sia modo di verificare il più possibile che la sua aderenza alla realtà permanga nel tempo. In termini più pratici, è necessario identificare le componenti del sistema complessivo delle quali è possibile fidarsi e potersi avvalere di un meccanismo che permetta di verificare nel tempo le basi per la fiducia. In questo senso si comprende l'importanza sia di componenti "prodotto", sia di "politiche e procedure" che diano alto livello di affidabilità e, per questo, oggetto di certificazione. È proprio il processo sopra delineato che ci conduce all'esigenza pratica di certificazione e accreditamento, come elementi fondamentali della catena di fiducia che permette di costruire sistemi robusti, di identificare responsabilità, di misurare e verificare le garanzie di sicurezza che sono state realizzate. Ad esempio, un prodotto di sicurezza non sottoposto a un processo di certificazione accreditata, è una potenziale sorgente di insicurezza, proprio perché non c'è garanzia che sia sottoposto a un processo, strutturato e costantemente aggiornato, di valutazione tecnica sulle possibili vulnerabilità. Tale rischio si attenua se il prodotto è certificato in accordo ad uno standard riconosciuto, ma rimane aperto un quesito. Quale soggetto ha certificato il prodotto? Che garanzie di fiducia esistono rispetto a questo soggetto? L'accreditamento è un modo convincente per rispondere a questo quesito, attraverso la migrazione della fiducia verso l'Ente di accreditamento che, per ruolo e responsabilità, dovrà avere caratteristiche adeguate a offrire tale fiducia. Accreditamento significa competenza e trasparenza, anche attraverso monitoraggio e implementazione di meccanismi di verifica pubblica (si pensi per esempio all'accreditamento degli organismi di certificazione che svolgono il processo di valutazione istruttoria, necessaria alla qualifica dei prestatori di servizi fiduciari in ambito eIDAS).

---

[27] Il concetto di "adeguatezza" va riferito al tipo di minacce alle quali può essere esposta un'infrastruttura, alla sua robustezza già esistente, al tipo e al valore delle informazioni gestite e ad altri parametri che suggeriscono una "personalizzazione" delle misure di controllo operativo diverse caso per caso.

[28] Con l'adozione di un ISMS si adottano misure di sicurezza delle informazioni e di cybersicurezza, cioè misure relative alla protezione delle informazioni sia nel perimetro aziendale, sia nello spazio di comunicazione dei dati, che viene spesso chiamato ciberspazio.

Accreditamento, in senso lato, significa rendere fruibile ed efficace l'adozione delle misure di sicurezza. Su questa consapevolezza e con l'obiettivo di dare ad essa ulteriore enfasi e supporto, si fonda il presente rapporto, la cui esigenza è sia legata alla ancora diffusa percezione che certificazione, rispetto di standard e norme e accreditamento in ambito di cybersecurity siano pesanti sovrastrutture burocratiche, sia legata alla mancanza di studi che provino a evidenziare il ruolo concreto di tali processi ed i benefici che essi apportano. Dopo la disamina del panorama normativo, attraverso i casi di studio e l'attività sul campo, il rapporto raggiunge questo obiettivo, attraverso diverse conclusioni che rappresentano i risultati proprio della ricerca effettuata. Al di là di numerosi aspetti di rilievo che la lettura dettagliata del rapporto può offrire al lettore, è utile evidenziare le principali considerazioni che si possono trarre dai risultati dell'analisi effettuata.

- Un primo aspetto da porre in evidenza è il fatto che i casi di studio analizzati hanno evidenziato un significativo grado di maturità del campione selezionato circa la consapevolezza del rischio informatico e i benefici apportati dal processo di certificazione ISO/IEC 27001 (certificazione a cui ci si è riferiti nell'attività di analisi in questione). Tuttavia, la piena acquisizione di questa consapevolezza ha richiesto del tempo, non solo perché identificare gli elementi che permettono di percepire i benefici non è immediato, ma anche perché essi derivano da dinamiche complesse, che sono appunto quelle che l'analisi condotta aveva l'obiettivo di mettere in luce. Così come è certamente di interesse il fatto che sia emerso con chiarezza quanto la certificazione ISO/IEC 27001 abbia rappresentato un elemento trainante per la postura dell'organizzazione rispetto al tema della conformità a norme, standard e regolamenti, in un'accezione più generale di quella che riguarda lo specifico standard considerato.

- Altro aspetto di rilievo che è risultato dallo studio è la diversificazione degli approcci utilizzati per l'adozione dello standard in funzione delle caratteristiche dell'organizzazione. L'analisi di tale aspetto permette infatti di avere utili informazioni circa le strategie di adozione dello standard, il loro grado di incrementabilità, l'identificazione dei contesti limitati in cui avviare la fase pilota, le strategie di migrazione. In altri termini, è apparso particolarmente interessante osservare come l'approccio che lo stesso standard ISO prevede, basato sul ciclo di Deming (*plan-do-check-act*), si traduca in azioni concrete nei casi analizzati e come queste varino in funzione delle caratteristiche dell'organizzazione (in particolare la dimensione e la diversificazione delle funzioni).

- L'attività condotta sul campo, attraverso la realizzazione di un vulnerability assessment di servizi esposti sul web, ha fornito ulteriori risultati significativi. Pur non potendo in alcun modo rappresentare un assessment di sicurezza esaustivo, un'attività di questo tipo fornisce senz'altro indizi molto chiari circa la postura di sicurezza dell'organizzazione, essendo proprio i servizi web quelli maggiormente sfruttati dagli attaccanti per assicurarsi un punto di ingresso nel perimetro dell'organizzazione. Il risultato ottenuto, che mostra una chiara correlazione tra la minore suscettibilità ad attacchi web delle organizzazioni certificate ISO/IEC 27001 rispetto a quelle certificate solamente a fronte della ISO 9001, non è irrilevante. Esso, infatti, rappresenta una misura in qualche modo quantitativa dei benefici della certificazione ISO/IEC 27001 e dimostra che, anche in un dominio caratterizzato da elevata attenzione verso la qualità di processo (dominio identificato dalla certificazione ISO 9001), non si sviluppa sufficiente attenzione verso la cybersecurity, né adeguate capacità di gestione della stessa.

In conclusione, lo studio descritto in questo rapporto, oltre ad offrire al lettore un punto di vista ampio e diversificato della certificazione e dell'accreditamento in ambito di cybersecurity e tutela dei dati personali, fornisce utili elementi di prova a supporto del principio che ha animato lo studio stesso, principio secondo il quale certificazione e accreditamento rappresentano fattori abilitanti per la cybersecurity e che esercitano un ruolo determinante nell'attuale processo di trasformazione digitale della società.

Riferimenti bibliografici

[2.1] Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo al ENISA, l'Agenzia dell'Unione europea per la cybersecurity, e alla certificazione della cybersecurity per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 («regolamento sulla cybersecurity»).
https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32019R0881&from=IT

[2.2] Centro studi del Senato della Repubblica e della Camera dei Deputati. Disposizioni urgenti in materia di cybersecurity, definizione dell'architettura nazionale di cybersecurity e istituzione dell'Agenzia per la cybersecurity nazionale. D.L. 82/2021 – A.C. 3161-A. Dossier del 23 luglio 2021.
http://documenti.camera.it/leg18/dossier/pdf/D21082a.pdf

[2.3] Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione.
https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:32016L1148&from=EN

[2.4] Proposta di Direttiva del Parlamento europeo e del Consiglio relativa a misure per un livello comune elevato di cybersecurity nell'Unione, che abroga la direttiva (UE) 2016/1148.
https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:52020PC0823&from=EN

[2.5] Decreto Legislativo 18 maggio 2018, n. 65 Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione.
www.gazzettaufficiale.it/eli/id/2018/06/09/18G00092/sg

[2.6] Decreto Legge 21 settembre 2019, n. 105 Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica.
https://www.gazzettaufficiale.it/eli/id/2019/09/21/19G00111/sg

[2.7] Legge 18 novembre 2019, n. 133 Conversione in legge, con modificazioni, del decreto-legge 21 settembre 2019, n. 105, recante disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica.
https://www.gazzettaufficiale.it/eli/id/2019/11/20/19G00140/sg

[2.8] Decreto del Presidente del Consiglio dei Ministri 30 luglio 2020, n. 131 Regolamento in materia di perimetro di sicurezza nazionale cibernetica, ai sensi dell'articolo 1, comma 2, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133.
https://www.gazzettaufficiale.it/eli/id/2020/10/21/20G00150/sg

[2.9] Decreto del Presidente del Consiglio dei Ministri 14 aprile 2021, n. 81 Regolamento in materia di notifiche degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici di cui all'articolo 1, comma 2, lettera b), del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, e di misure volte a garantire elevati livelli di sicurezza.
https://www.gazzettaufficiale.it/eli/id/2021/06/11/21G00089/sg

[2.10] Decreto del Presidente della Repubblica 5 febbraio 2021, n. 54 Regolamento recante attuazione dell'articolo 1, comma 6, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133.
https://www.gazzettaufficiale.it/eli/id/2021/04/23/21G00060/sg

[2.11] Decreto del Presidente del Consiglio dei Ministri 15 giugno 2021 Individuazione delle categorie di beni, sistemi e servizi ICT destinati a essere impiegati nel perimetro di sicurezza nazionale cibernetica, in attuazione dell'articolo 1, comma 6, lettera a), del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133.
https://www.gazzettaufficiale.it/eli/id/2021/08/19/21A05087/sg

[2.12] Decreto Legge 14 giugno 2021, n. 82 Disposizioni urgenti in materia di cybersecurity, definizione dell'architettura nazionale di cybersecurity e istituzione dell'Agenzia per la cybersecurity nazionale.
https://www.gazzettaufficiale.it/eli/id/2021/06/14/21G00098/sg

[2.13] Decreto del Presidente del Consiglio dei Ministri 30 ottobre 2003 Approvazione dello schema nazionale per la valutazione e la certificazione della sicurezza nel settore della tecnologia dell'informazione, ai sensi dell'art. 10, comma 1, del decreto legislativo 23 febbraio 2002, n. 10.
https://www.gazzettaufficiale.it/eli/id/2004/04/27/04A04314/sg

[2.14] Legge 4 agosto 2021, n. 109 Conversione in legge, con modificazioni, del decreto-legge 14 giugno 2021, n. 82, recante disposizioni urgenti in materia di cybersecurity, definizione dell'architettura nazionale di cybersecurity e istituzione dell'Agenzia per la cybersecurity nazionale.
https://www.gazzettaufficiale.it/eli/id/2021/08/04/21G00122/sg

[2.15] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).
https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:32016R0679&from=IT

[2.16] Decreto Legislativo 10 agosto 2018, n. 101 Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).
https://www.gazzettaufficiale.it/eli/id/2018/09/04/18G00129/sg

[2.17] Decreto Legislativo 196/2003. Codice in materia di protezione dei dati personali (Testo coordinato).
https://www.garanteprivacy.it/garante/doc.jsp?ID=9042678

[2.18] Circolare n. 285 del 17 dicembre 2013 Circolare n. 285, Banca d'Italia.
https://www.bancaditalia.it/compiti/vigilanza/normativa/archivio-norme/circolari/c285/

[2.19] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC.
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32015L2366

[2.20] EBA Guidelines on ICT and security risk management, EBA/GL/2019/04, 29 novembre 2019.
https://www.eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-ict-and-security-risk-management

[2.21] EBA Guidelines on outsourcing arrangements, EBA/GL/2019/02, 25 febbraio 2019
https://www.eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-outsourcing-arrangements

[2.22] EBA Revised Guidelines on major incident reporting under PSD2, EBA/GL/2021/03, 10 giugno 2021. https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2021/Guidelines%20on%20major%20incident%20reporting%20under%20PSD2%20EBA-GL-2021 03/Translations/1019014/Final%20revised%20Guidelines%20on%20major%20incident%20reporting%20under%20PSD2_IT_COR.pdf

[2.23] Cyber resilience oversight expectations for financial market infrastructures, European Central Bank, dicembre 2018. https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf

[2.24] Proposal for a Regulation of the European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014, 24 settembre 2020. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0595

[2.25] Regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE. https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX%3A32014R0910&from=EN

[2.26] Regolamento (CE) n. 765/2008 del Parlamento europeo e del Consiglio del 9 luglio 2008 che pone norme in materia di accreditamento e vigilanza del mercato per quanto riguarda la commercializzazione dei prodotti e che abroga il Regolamento (CEE) n. 339/93 https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:218:0030:0047:it:PDF

[2.27] UNI CEI EN ISO/IEC 27001:2017 Tecnologie Informatiche - Tecniche di sicurezza - Sistemi di gestione della sicurezza dell'informazione - Requisiti. https://store.uni.com/p/UNI1602960/uni-cei-en-isoiec-270012017-265673/UNI1602960_EEN

[2.28] Framework Nazionale per la Cybersecurity e la Data Protection, v. 2.0, febbraio 2019. https://www.cybersecurityframework.it/framework2

[2.29] Common Criteria (ISO/IEC 15408). https://www.commoncriteriaportal.org/cc/

[2.30] Decreto del Presidente del Consiglio dei Ministri 18 maggio 2022. Regolamento in materia di accreditamento dei laboratori di prova e di raccordi tra Centro di Valutazione e Certificazione Nazionale, i laboratori di prova accreditati e i Centri di Valutazione del Ministero dell'interno e del Ministero della Difesa, ai sensi dell'articolo 1, comma 7, lettera b), del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133. https://www.gazzettaufficiale.it/eli/id/2022/07/15/22G00099/sg

[2.31] ISO/IEC 17011:2017 Conformity assessment - Requirements for accreditation bodies accrediting conformity assessment bodies. https://www.iso.org/standard/67198.html

[2.32] UNI CEI EN ISO/IEC 17024:2012, Valutazione della conformità - Requisiti generali per organismi che eseguono la certificazione di persone.

[2.33] UNI 11621-1, Attività professionali non regolamentate - Profili professionali per l'ICT - Parte 1: Metodologia per la costruzione di profili professionali basati sul sistema e-CF;
UNI 11621-2, Attività professionali non regolamentate - Profili professionali per l'ICT - Parte 2: Profili professionali di "seconda generazione";
UNI 11621-3, Attività professionali non regolamentate - Profili professionali per l'ICT - Parte 3: Profili professionali relativi alle professionalità operanti nel Web;
UNI 11621-4, Attività professionali non regolamentate - Profili professionali per l'ICT - Parte 4: Profili professionali relativi alla sicurezza delle informazioni;
UNI 11621-5, Attività professionali non regolamentate - Profili professionali per l'ICT -

Parte 5: Profili professionali relativi all'informazione geografica.

[2.34] UNI 11506:2021, Attività professionali non regolamentate - Figure professionali operanti nel settore ICT - Requisiti per la valutazione della conformità delle conoscenze, abilità, autonomia e responsabilità per i profili professionali ICT basati sul modello e-CF. https://store.uni.com/p/UNI1608578/uni-115062021-309903/UNI1608578_EIT

[2.35] UNI EN 16234-1 e-Competence Framework (e-CF) - Framework comune europeo per i professionisti ICT in tutti i settori - Parte 1: Framework (modello di riferimento). https://www.uni.com/index.php?option=com_content&view=article&id=9985%3Ae-competence-framework&catid=170&Itemid=2612

[2.36] Decreto Legislativo 16 gennaio 2013, n. 13 Definizione delle norme generali e dei livelli essenziali delle prestazioni per l'individuazione e validazione degli apprendimenti non formali e informali e degli standard minimi di servizio del sistema nazionale di certificazione delle competenze, a norma dell'articolo 4, commi 58 e 68, della legge 28 giugno 2012, n. 92. https://www.gazzettaufficiale.it/eli/id/2013/02/15/13G00043/sg

[2.37] CWA 16458-1:2018 European ICT professionals role profiles - Part 1: 30 ICT profiles. https://store.uni.com/cwa-16458-1-2018

[3.1] SPARTA (EU H2020 Project), International and national cybersecurity certification initiatives, 3 Febbraio 2020. https://www.sparta.eu/assets/deliverables/SPARTA-D11.1-International-and-national-cybersecurity-certification-initiatives-PU-M12.pdf

[3.2] Securing the Future of Payments: PCI SSC Publishes PCI Data Security Standard v4.0. PCI Security Standards Council. March 31, 2022. https://www.pcisecuritystandards.org/about_us/press_releases/securing-the-future-of-payments-pci-ssc-publishes-pci-data-security-standard-v4-0/

[3.3] OWASP Web Security Testing Guide. OWASP, 2022. https://owasp.org/www-project-web-security-testing-guide/

[3.4] ISO/SAE 21434:2021: Road vehicles - Cybersecurity engineering, 2021. https://www.iso.org/standard/70918.html#:~:text=This%20document%20specifies%20engineering%20requirements,including%20their%20components%20and%20interfaces.

[5.1] ISECOM, “Open Source Security Testing Methodology Manual”, versione 3. https://www.isecom.org/OSSTMM.3.pdf

[5.2] Open Web Application Security Project (OWASP), "OWASP Application Security Verification Standard". https://owasp.org/www-project-application-security-verification-standard/

[5.3] Open Web Application Security Project (OWASP), “Web Security Testing Guide”. https://owasp.org/www-project-web-security-testing-guide/

[5.4] Gazzetta ufficiale dell'Unione europea, L124/36 del 20/05/2013, “Raccomandazione della Commissione del 6 maggio 2003 relativa alla definizione delle microimprese, piccole e medie imprese”. https://www.mise.gov.it/images/stories/documenti/Raccomandazione-6-5-2003-definizione-pmi.pdf

[5.5] Istituto Nazionale di Statistica, Territorio, 2017. https://www.istat.it/it/files/2017/12/C01.pdf

[5.6] Sedgwick, Philip. "Convenience sampling." Bmj 347 (2013).

[5.7] “CMSeek - CMS Detection & Exploitation Suite”. https://github.com/Tuhinshubhra/CMSeeK

[5.8] "Testssl.sh".
https://testssl.sh

[5.9] "WPScan WordPress security".
https://github.com/wpscanteam/wpscan

[5.10] "OWASP Joomla Vulnerability Scanner Project".
https://github.com/OWASP/joomscan

[5.11] National Institute of Standards and Technology, NAtional Vulnerability Database.
https://nvd.nist.gov

[5.12] Shodan, Shodan Search Engine.
https://www.shodan.io

[5.13] Computer Emergency Response Team (AGID), "Uno sguardo ai server della Pubblica Amministrazione attraverso i dati di Shodan", 2021.
https://cert-agid.gov.it/news/mappatura-delle-vulnerabilita-della-pubblica-amministrazione-mediante-fonti-osint/

[5.14] Computer Emergency Response Team (AGID), "Monitoraggio sul corretto utilizzo del protocollo HTTPS e dei livelli di aggiornamento delle versioni dei CMS nei portali Istituzionali della PA", 2021.
https://cert-agid.gov.it/news/monitoraggio-sul-corretto-utilizzo-del-protocollo-https-e-dei-livelli-di-aggiornamento-delle-versioni-dei-cms-nei-portali-istituzionali-della-pa/

[5.15] Computer Emergency Response Team (AGID), "Secondo monitoraggio dello stato di aggiornamento del protocollo HTTPS e dei CMS sui sistemi della PA.", 2021.
https://cert-agid.gov.it/news/secondo-monitoraggio-dello-stato-di-aggiornamento-del-protocollo-https-e-dei-cms-sui-sistemi-della-pa/

[5.16] MITRE Corporation, Common Vulnerabilities Exposure.
https://cve.mitre.org

[5.17] Forum of Incident Response and Security Teams, Common Vulnerability Scoring System.
https://www.first.org/cvss/

[5.18] Synopsys, The Heartbleed Bug.
https://heartbleed.com

[5.19] Internet Assigned Numbers Authority, Transport Layer Security (TLS) Parameters, 2005,
https://www.iana.org/assignments/tls-parameters/tls-parameters.xml#tls-parameters-3

[5.20] Mozilla, Security/Server Side TLS, 2022.
https://wiki.mozilla.org/Security/Server_Side_TLS

[5.21] SSLLabs, SSL Server Rating Guide.
https://github.com/ssllabs/research/wiki/SSL-Server-Rating-Guide

[5.22] Wappalyzer.
https://www.wappalyzer.com

[5.23] Raccomandazioni Agid in merito allo standard Transport Layer Security (TLS).
https://cert-agid.gov.it/wp-content/uploads/2020/11/AgID-RACCSECTLS-01.pdf

[5.24] Strict-Transport-Security - HTTP | MDN.
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security

[5.25] OWASP Foundation.
https://owasp.org

[5.26] Testing for Weak Transport Layer Security.
https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/09-Testing_for_Weak_Cryptography/01-Testing_for_Weak_Transport_Layer_Security

[5.27] Joomla!
https://www.joomla.org

[6.1] Centro Criptológico Nacional (CCN). Metodología de Evaluación para la Certificación Nacional Esencial de Seguridad (LINCE), 2002.
https://www.ccn.cni.es/index.php/en/menu-news-ccn-en/567-el-centro-criptologico-nacional-publica-una-guia-con-la-metodologia-de-evaluacion-lince

[6.2] Agence nationale de la sécurité des systèmes d'information (ANSSI). ANSSI-CSPN-CER-P-01 First level security certification for information technology products – v1.1, 2020.
https://www.ssi.gouv.fr/administration/produits-certifies/cspn/les-procedures-formulaires-et-methodologies/

[6.3] Bundesamt für Sicherheit in der Informationstechnik (BSI). Accelerated Security Certification (BSZ), 2021.
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/Anerkennung-von-Stellen-und-Zertifizierung-IT-Sicherheitsdienstleister/BSZ/bsz_node.html

[6.4] Algemene Inlichtingen- en Veiligheidsdienst (AIVD). Baseline Security Product Assessment, 2020.
https://www.aivd.nl/onderwerpen/informatiebeveiliging/documenten/publicaties/2020/07/15/nbv-brochure-bspa

[6.5] European Cyber Security Organization (ECSO). POSITION PAPER - Initial position on the EU cybersecurity package, 2017.
https://www.ecs-org.eu/publications

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