UNINDUSTRIA
UNIONE DEGLI INDUSTRIALI E DELLE IMPRESE
ROMA • FROSINONE • LATINA • RIETI • VITERBO

CONFINDUSTRIA SERVIZI
INNOVATIVI E TECNOLOGICI

Posteitaliane

AGENZIA PER LA CYBERSICUREZZA NAZIONALE
ACN
SAPIENTIA ADIUVAT

ACCREDIA
L'ENTE ITALIANO DI ACCREDITAMENTO

CYBERSECURITYREADINESS.IT

Cyber Security Readiness

European
DIGITAL SME
Alliance

UNIVERSITÀ CAMPUS BIO-MEDICO DI ROMA

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

CIS SAPIENZA
RESEARCH CENTER OF CYBER INTELLIGENCE
AND INFORMATION SECURITY

cini
consorzio
interuniversitario
nazionale
per l'informatica

LUISS

SERICS
SECURITY AND RIGHTS IN THE CYBERSPACE

Contesto

- Negli ultimi anni, **l’incremento esponenziale degli attacchi cibernetici**, unito all’ampio utilizzo di soluzioni cloud e Internet of Things (IoT), ha reso la sicurezza informatica un’emergenza globale. Questa preoccupazione coinvolge sia le aziende che le autorità di tutti i paesi.

- Le **valutazioni e certificazioni della sicurezza dei prodotti ICT** svolgono un ruolo cruciale in questo settore. **Garantiscono agli utenti** che tali prodotti hanno implementato le necessarie misure di sicurezza e sono stati testati per verificare l’efficacia di queste misure contro vulnerabilità note.

- **Per i fornitori di prodotti ICT e gli acquirenti**, è fondamentale **eliminare le vulnerabilità dai propri prodotti**. Questo riduce la possibilità di sfruttarle per attaccare il prodotto.

FORMAZIONE & AWARENESS

RESILIENZA

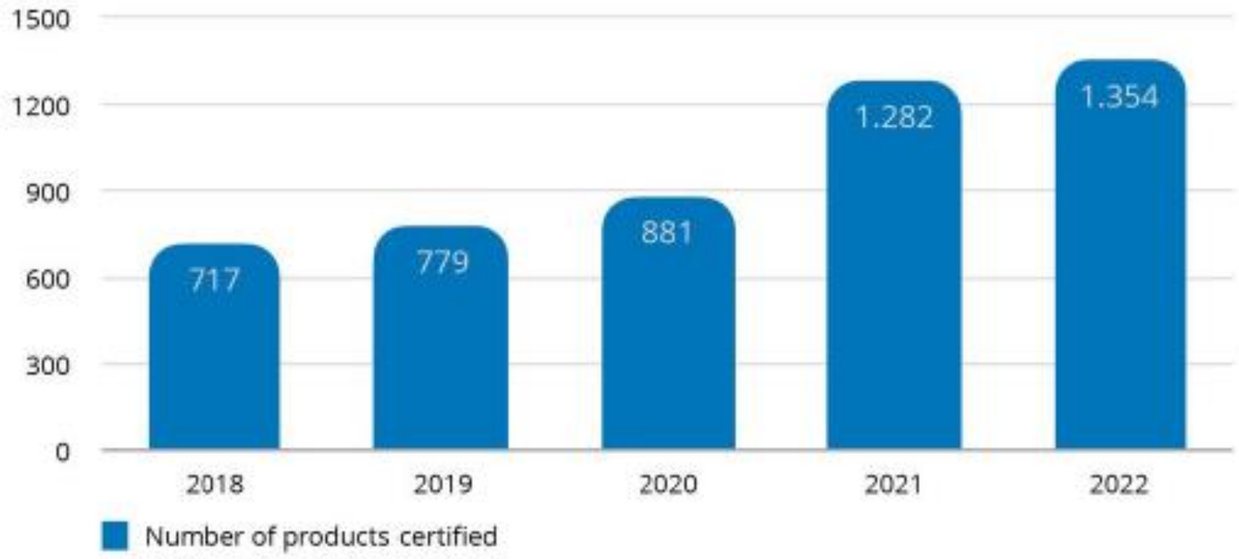
Ecosistemi, RETI e ISAC

Contesto

- Per quanto riguarda i prodotti TIC (Tecnologie dell'Informazione e della Comunicazione), si può osservare che il **numero di schemi e metodologie di valutazione è in crescita** nel corso degli anni.

- Il mercato della valutazione della cybersecurity per i prodotti ICT **non si basa solo sui Common Criteria**, sono nati nuovi schemi per rispondere a esigenze settoriali, come i pagamenti, le telecomunicazioni o i trasporti, le tecnologiche, in generale per **l'aumento dei dispositivi connessi**.

- Come mostrato nella Figura, la crescita è stata significativa negli ultimi 3 anni, in particolare tra il 2020 e il 2021. Tuttavia, la crescita tra il 2021 e il 2022 non è così notevole. (dato da analizzare se dovuto ad influenza del COVID).



Evoluzione quinquennale a livello mondiale del numero totale di prodotti ICT approvati o certificati, combinando tutte le valutazioni sulla sicurezza informatica del rapporto

https://www.enisa.europa.eu/publications/cybersecurity-market-assessments

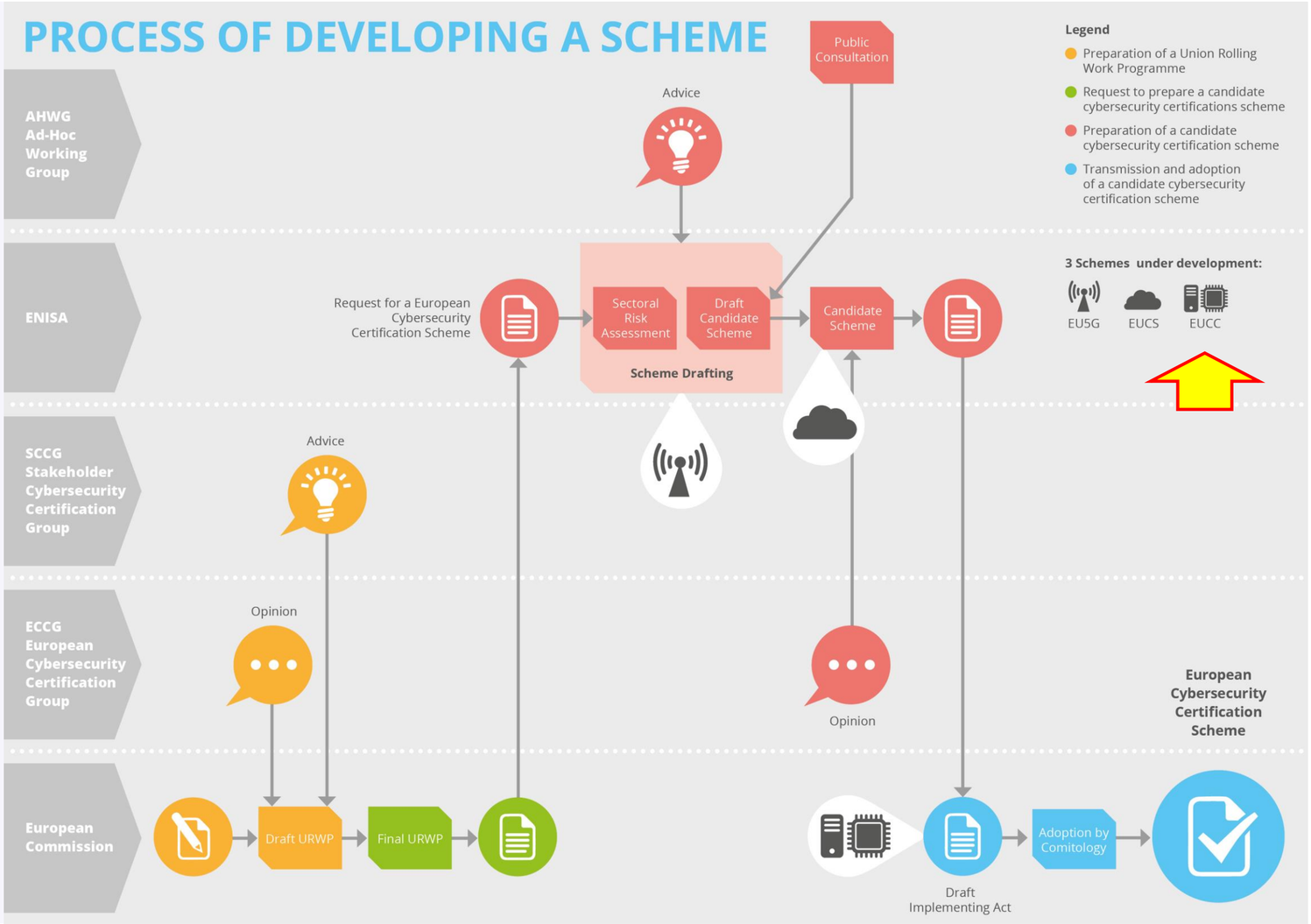
Contesto

Certificazione UE per la cybersicurezza
Porta fiducia nel mercato dei prodotti, dei servizi e dei processi ICT in tutta l'Unione e oltre.

- Lo scorso 31 gennaio 2024 **è stato adottato il primo sistema di certificazione** (Atto di Esecuzione) di cybersecurity a livello europeo: **lo European Union Cybersecurity Certification (EUCC) Scheme on Common Criteria**. Il primo sistema, riguarda i prodotti TIC come i prodotti e i componenti hardware e software.

- Per quanto riguarda i Common Criteria per i prodotti ICT, il 44% del totale degli organismi di valutazione si trova in Europa.

- Il sistema **si basa sul collaudato quadro di valutazione dei criteri comuni SOG-IS** ("Senior Officials Group Information Systems Security"), già utilizzato in 17 Stati membri dell'UE.



https://certification.enisa.europa.eu/

Contesto

Gazzetta ufficiale dell'Unione europea

IT
Serie L

2024/482

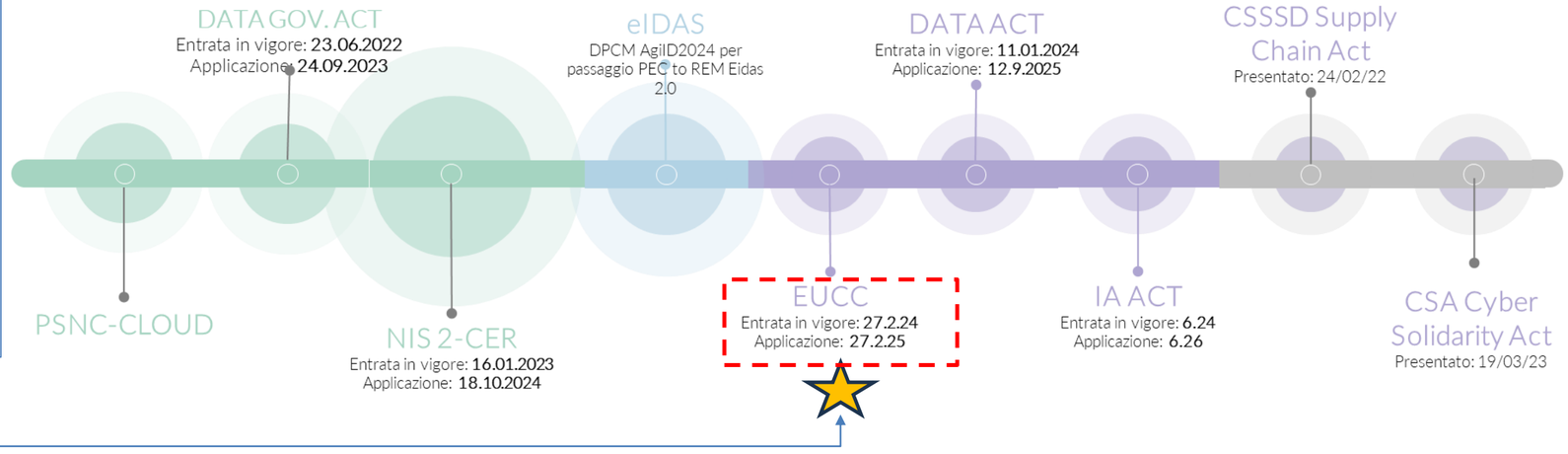
7.2.2024

REGOLAMENTO DI ESECUZIONE (UE) 2024/482 DELLA COMMISSIONE

del 31 gennaio 2024

recante modalità di applicazione del regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio per quanto riguarda l'adozione del sistema europeo di certificazione della cibersicurezza basato sui criteri comuni (EUCC)

(Testo rilevante ai fini del SEE)



- **Atto di Esecuzione**

(1) Il presente regolamento specifica i **ruoli, le norme e gli obblighi, nonché la struttura del sistema europeo di certificazione della cibersicurezza** basato sui criteri comuni (**European Common Criteria-based cybersecurity certification – EUCC**) in conformità del quadro europeo di certificazione della cibersicurezza di cui al regolamento (UE) 2019/881. L'EUCC si fonda sull'accordo sul reciproco riconoscimento (ARR) dei certificati di valutazione della sicurezza delle tecnologie dell'informazione del gruppo di alti funzionari competente in materia di sicurezza dei sistemi d'informazione (Senior Officials Group – Information Systems Security, SOG-IS) e si basa sui criteri comuni, comprese le procedure e i documenti del gruppo.

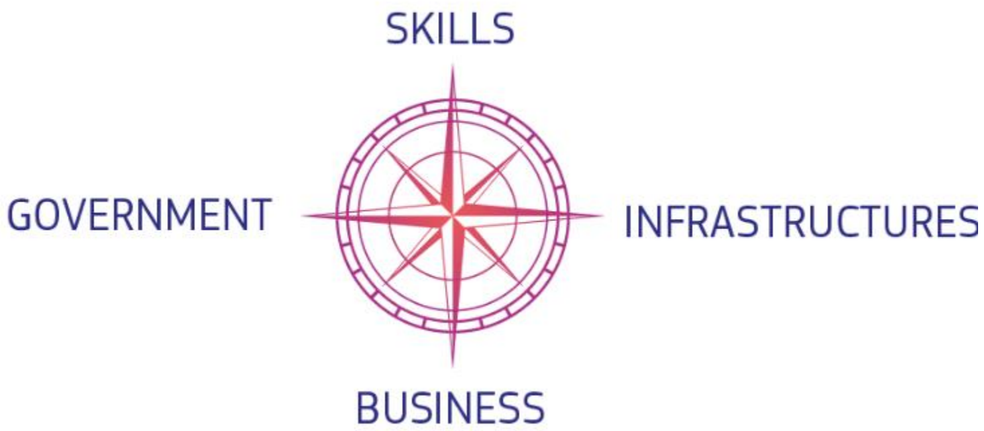
(2) Il sistema dovrebbe basarsi su **norme internazionali consolidate**. I criteri comuni (**Common Criteria**) sono una norma internazionale per la valutazione della sicurezza delle informazioni pubblicata, ad esempio, come ISO/IEC 15408 Information security, cybersecurity and privacy protection — Evaluation criteria for IT security. Essa si basa sulla valutazione da parte di terzi e prevede sette livelli di garanzia della valutazione (Evaluation Assurance Level – EAL). I criteri comuni sono accompagnati dalla metodologia comune di valutazione (Common Evaluation Methodology), pubblicata, ad esempio come ISO/IEC 18045 - Information security, cybersecurity and privacy protection - Evaluation criteria for IT security - Methodology for IT security evaluation. Le specifiche e i documenti che applicano le disposizioni del presente regolamento possono riferirsi a una norma disponibile al pubblico che rispecchia la norma utilizzata per la certificazione nel quadro del presente regolamento, ad esempio i criteri comuni per la valutazione della sicurezza delle tecnologie dell'informazione (Common Criteria for Information Technology Security Evaluation) e la metodologia comune per la valutazione della sicurezza delle tecnologie dell'informazione (Common Methodology for Information Technology Security Evaluation).

(10) Al fine di garantire un **elevato livello di fiducia e affidabilità dei prodotti TIC certificati**, a norma del presente regolamento non dovrebbe essere consentita l'autovalutazione. Dovrebbe essere consentita solo la **valutazione di conformità da parte di terzi effettuata dalle strutture di valutazione della sicurezza delle tecnologie** dell'informazione (Information Technology Security Evaluation Facilities – ITSEF) e dagli organismi di certificazione.

Contesto – il Mercato UE

Oltre 760 milioni di EUR di investimenti dal programma Europa digitale per la transizione digitale e la cibersicurezza dell'Europa

La Commissione ha adottato i programmi di lavoro modificati per il 2024 per il programma Europa digitale, che delineano gli obiettivi e i settori tematici specifici che riceveranno un finanziamento totale di 762.7 milioni di EUR



Europe’s Digital Decade: digital targets for 2030

Perché serva Portare fiducia nel mercato dei prodotti, dei servizi e dei processi ICT in tutta l'Unione.

Un'economia in crescita

Dal 2018 al 2025:

- il valore dell'economia dei dati nell'UE-27 dovrebbe passare da 301 miliardi di EUR a **829 miliardi di** EUR
- il numero di professionisti dei dati aumenterà da 5,7 milioni a 10,9 milioni
- la popolazione dell'UE con competenze di base aumenterà dal 57% al 65%

SVILUPPARE IL MERCATO

PROTEGGERE I CITTADINI (LE INFRASTRUTTURE CRITICHE)

Oltre 760 milioni di EUR di investimenti dal programma Europa digitale per la transizione digitale e la cibersicurezza dell'Europa | Plasmare il futuro digitale dell'Europa
Europe’s digital decade: 2030 targets | European Commission (europa.eu)
Un futuro digitale per l'Europa - Consilium

Contesto – dispositivi connessi

2028: si prevede che nel mondo circa il 33% delle case saranno dotate di dispositivi connessi

2028: ci sono al momento oltre 300 milioni di auto connesse e si prevede che questo numero potrà salire entro il 2028 a circa 800 milioni mezzi

Oggi oltre 6 miliardi di smart phone sono attivi nel mondo (>46 milioni in Italia)

In circolazione attualmente 1,1 miliardi di dispositivi

Il mercato nel 2022 aveva un valore di circa 22 miliardi $

Il mercato degli assistenti vocali avrà un valore stimato di circa 20 miliardi $ nel 2028

Dispositivi per la casa intelligente:
- Termostati intelligenti
- Serrature intelligenti
- Campane per porte video intelligenti
- Lampadine intelligenti
- Prese intelligenti
- Aspirapolvere robotizzati

Elettrodomestici connessi:
- Frigoriferi intelligenti
- Forni intelligenti
- Lavatrici intelligenti
- Macchine da caffè intelligenti

Dispositivi indossabili:
- Smartwatch
- Braccialetti per il fitness
- Occhiali intelligenti
- Indumenti connessi

Assistenti vocali e altoparlanti intelligenti:
- Amazon Echo (Alexa)
- Google Home (Assistant)
- Apple HomePod (Siri)

Sicurezza e sorveglianza:
- Telecamere di sicurezza intelligenti
- Sensori di movimento
- Sistemi di allarme connessi

Salute e benessere:
- Bilance intelligenti
- Monitor per la pressione sanguigna
- Glucometri connessi

Sistemi di irrigazione e giardinaggio intelligenti:
- Controlli dell'irrigazione connessi
- Sensori di umidità del suolo

Automobile e trasporti:
- Sistemi di navigazione connessi
- Diagnostica veicolare remota
- Chiavi digitali

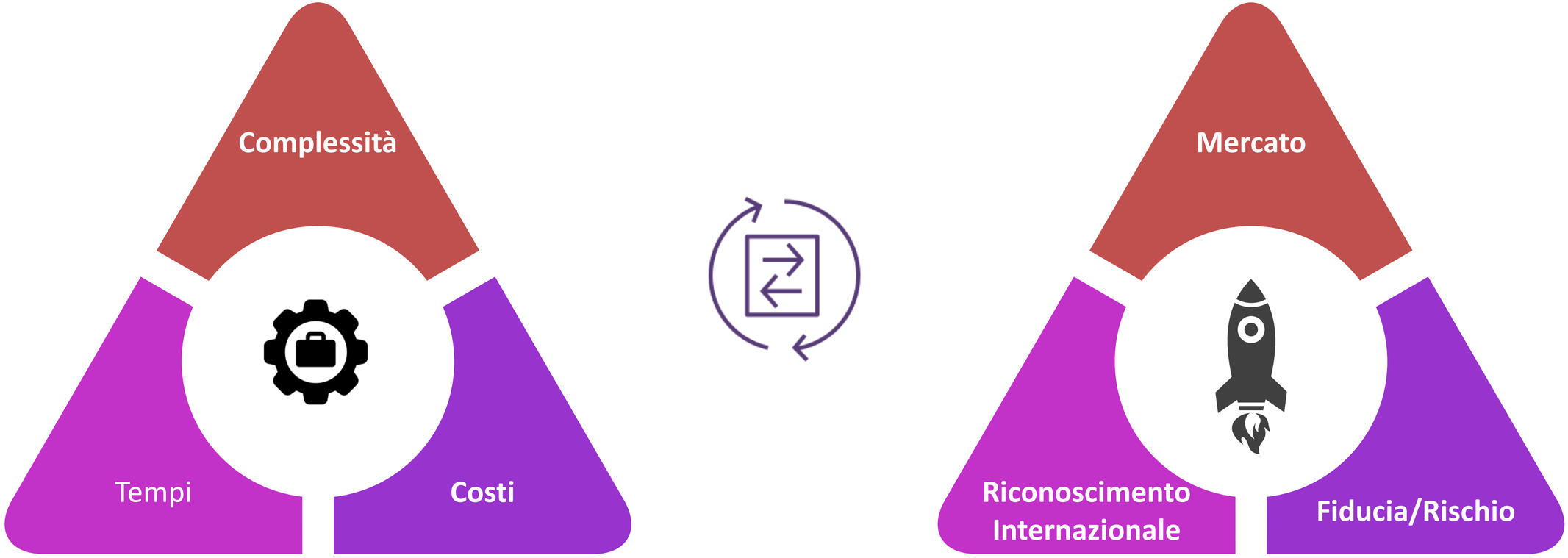
Industria e produzione (IIoT - Industrial Internet of Things):
- Sensori industriali (temperatura, pressione, vibrazioni.)
- Robot connessi per l'automazione della produzione
- Sistemi di gestione dell'energia

Infrastrutture urbane e gestione dell'energia:
- Contatori intelligenti (elettricità, gas, acqua)
- Illuminazione pubblica intelligente
- Sistemi di monitoraggio del traffico

Le certificazioni: una sfida utile per lo sviluppo del Mercato

Le **metodologie per la certificazione** di un prodotto **possono essere complesse per una PMI** (questo vale tanto per le certificazioni di prodotto quanto per le certificazioni di Sistema).

- ❑ Devono essere approcciate con consapevolezza rispetto al percorso ed agli impegni necessary;
- ❑ Può in generale essere efficace, dove possible, un approccio progressive;
- ❑ Forte Commitment.



Metodologia CSR: il Processo in 4 step

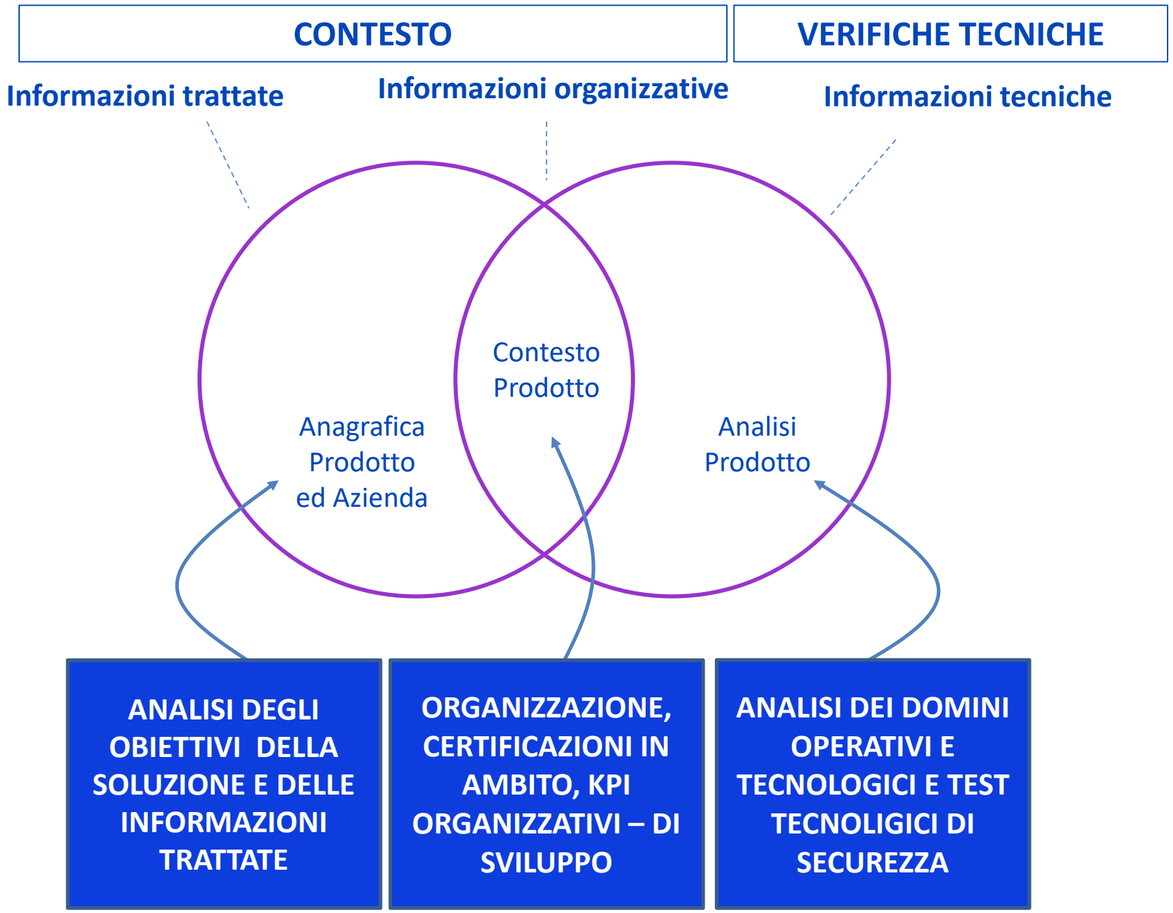
Il CSR **ha definito una propria metodologia** che ha come obiettivo quello di **supportare le PMI** nel comprendere quanto possono essere “distanti/Maturi” dal poter affrontare un percorso di certificazione del prodotto.
In generale la Metodologia del CSR vuole valutare le Misure di sicurezza che sono integrate nella soluzione/prodotto, e quanto il prodotto e l’organizzazione hanno sviluppato un percorso di applicazione delle best practice di Sicurezza.

Metodologia CSR: Avvio delle prime 2 fasi del Processo

In questa fase saranno avviate dal CSR solo le prime 2 fasi del Processo

Metodologia CSR

Il **modello** ha l'obiettivo di **supportare le PMI nel comprendere quanto il loro prodotto/organizzazione possano essere «maturi» per avviare un percorso di certificazione.**

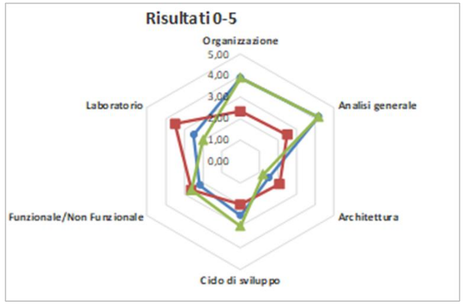


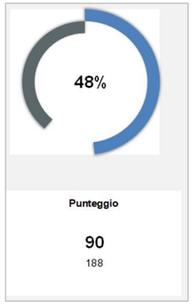
Il Framework si impegna a **garantire il raggiungimento di una valutazione** della soluzione oggetto dell'analisi, attraverso **6 DOMINI**

Metodologia CSR

DOMINI

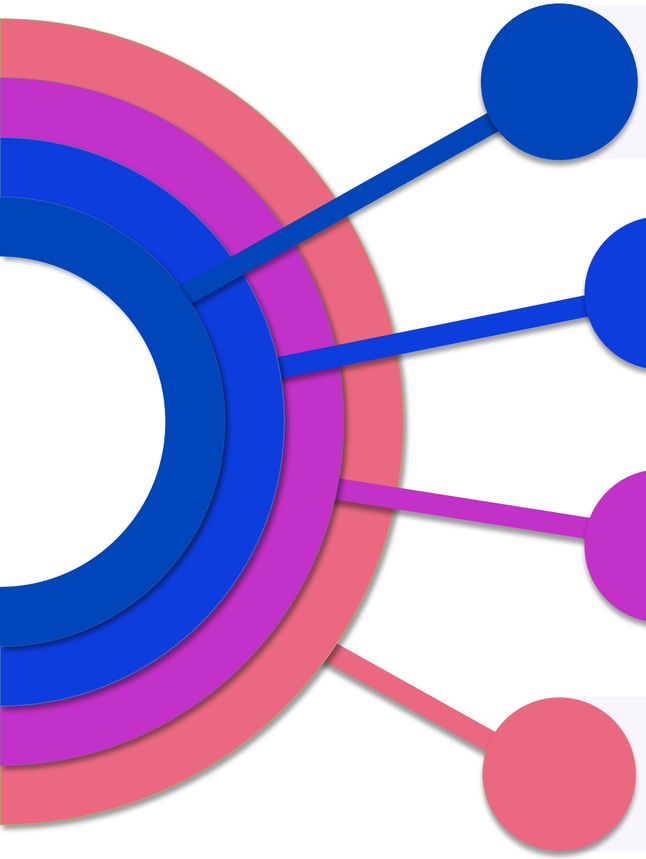
Organizzazione	Soluzione e livello di Maturità	Architettura e soluzioni Tecnologiche	Ciclo di vita del prodotto	Analisi Funzionale/Non Funzionale	Test ed Analisi Laboratorio
Valutazione Dominio	Valutazione Dominio	Valutazione Dominio	Valutazione Dominio	Valutazione Dominio	Valutazione Dominio
0 1 2 3 4 5	0 1 2 3 4 5	0 1 2 3 4 5	0 1 2 3 4 5	0 1 2 3 4 5	0 1 2 3 4 5





Metodologia CSR – Dominio Organizzazione

Si osserva l'Organizzazione, e le sue principali Dimensioni (dimensione, certificazioni, organizzazione e processi, team dedicati al prodotto, risultanze degli audit, eventuali incidenti avvenuti, etc.)



DIMENSIONI AZIENDALE

Si analizza la dimensione aziendale in termini di fatturato e numero di dipendenti e rapportando questi elementi agli indicatori relative il Prodotto

MERCATO

Si analizza il mercato della soluzione, con un focus sull'area geografica dei client per comprendere il suo sviluppo

BREVETTI

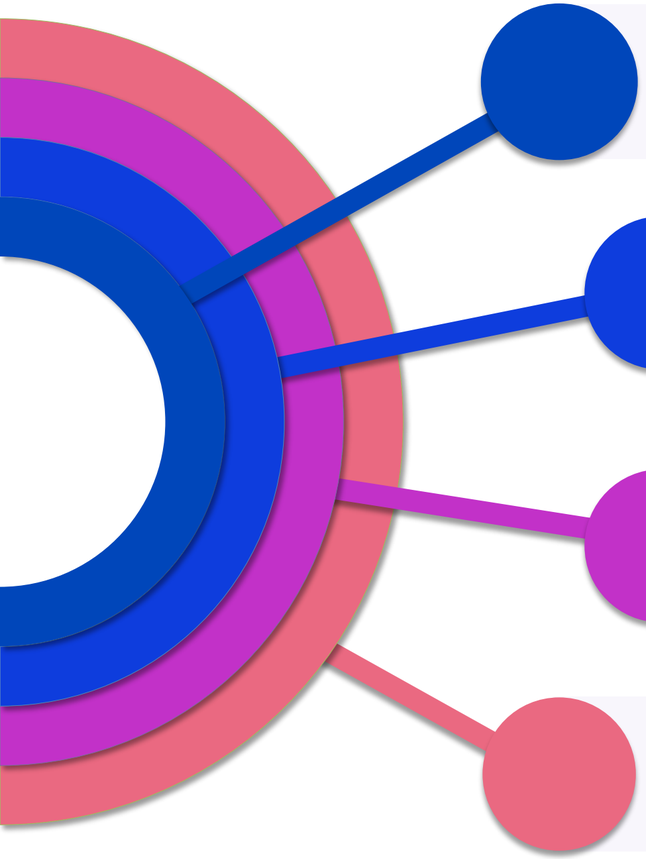
Si analizza la presenza di soluzioni per le quali sono stati depositati dei brevetti

CERTIFICAZIONI

Si analizzano le principali certificazioni in ambito, con particolare focus su quelle legate a specifici settori Industriali, trattamento delle informazioni/dati, Sistemi di Gestione

Metodologia CSR – Dominio Soluzione e livello di Maturità

Si osserva il percorso di Maturità della soluzione. Identificazione della soluzione e del perimetro (target), anagrafica, anni di vita, numero release, roadmap, interventi evolutivi migliorativi, scopo della soluzione, documentazione della soluzione e relativa manualistica, etc.



VITA DELLA SOLUZIONE

Si analizza da quanto tempo la soluzione è presente sul mercato, il numero di release rilasciate e la loro complessità

BUG & FIX

Si analizzano i principali bug riscontrati e le correttive messe in atto

ROADMAP EVOLUTIVA

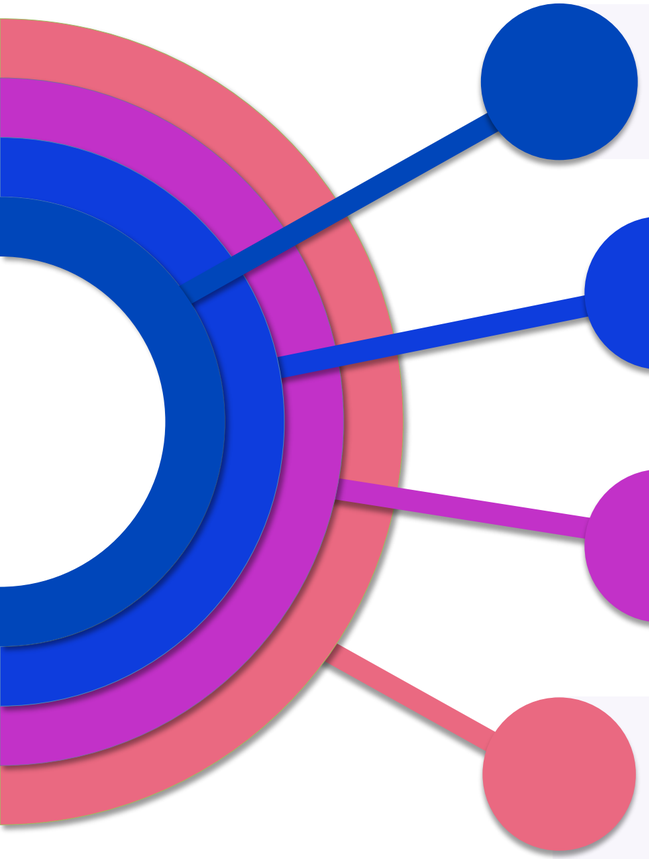
Si analizza la roadmap di evoluzione della soluzione, il piano degli interventi evolutivi, l'efficacia implementativa

EROGAZIONE DEL SERVIZIO

Si analizza le modalità di erogazione del servizio, in particolare il supporto che viene fornito al cliente, la completezza della documentazione, la presenza di specifici programmi formativi

Metodologia CSR – Dominio Architettura e soluzioni Tecnologiche

Si osserva l'Architettura della soluzione, le sue componenti e le scelte tecnologiche adottate (soluzioni e moduli software sviluppati e/o di terze parti, moduli cifratura, componenti, etc.), i requisiti di sicurezza in perimetro, la valutazione dei rischi effettuata.



PRODOTTI UTILIZZATI

Si analizza le soluzioni tecnologie impiegate per il servizio, vengono classificati i prodotti Open Souce, Custom, Commerciali, vengono censiti i linguaggi e le librerie utilizzate

MODALITA' DI EROGAZIONE

Si verifica la modalità di erogazione del servizio (SaaS, on premises, etc.) ed il disegno architetturale della soluzione

MISURE DI SICUREZZA

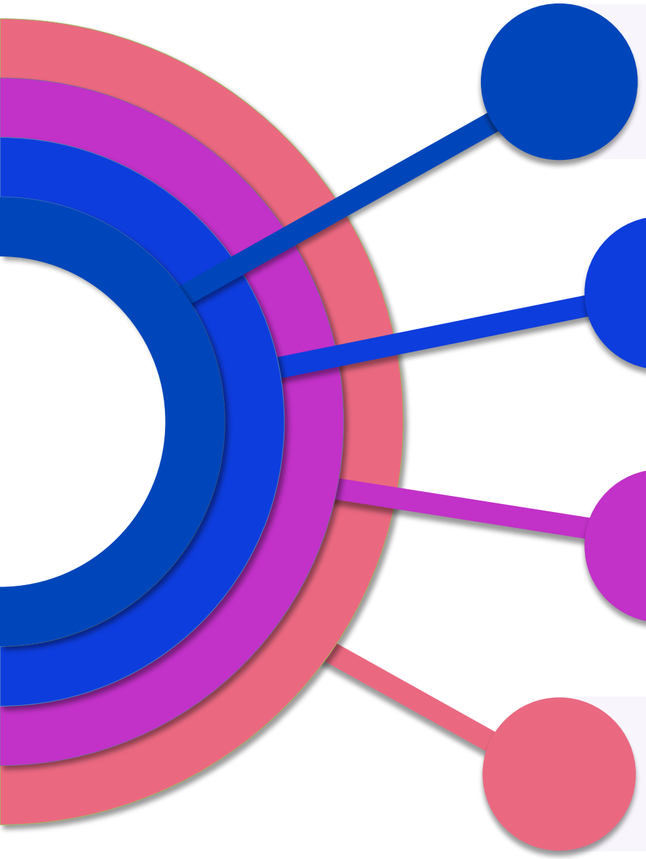
Si verificano i presidi di Sicurezza posti in essere, e il rispetto della logica di Security By Design

ANALISI DEI RISCHI

Si verificano i prinicipali rischi presi in considerazione dall'organizzazione, si analizzano eventuali incidenti ed anomalie con un focus sulle tempistiche per il ripristino dei servizi e dell'impatto generale causato (in modo assolutamente anonimo rispetto le Terze Parti).

Metodologia CSR – Dominio Ciclo di vita del prodotto

Si osserva la realizzazione della soluzione ed il ciclo di vita adottato (impiego di standard e Best-Practice, documentazione prodotta, aggiornamenti al prodotto, vulnerabilità/mal funzionamenti, supporto fornito al cliente, etc.).



STANDARD/BEST PRACTICE

Si verifica se durante l'intero ciclo di vita della soluzione sono impiegati specifici standard/best practice, strumenti di lavoro, etc.

DOCUMENTAZIONE AMMINISTRATIVA

Si verifica se la documentazione amministrativa prodotta è completa ed aggiornata

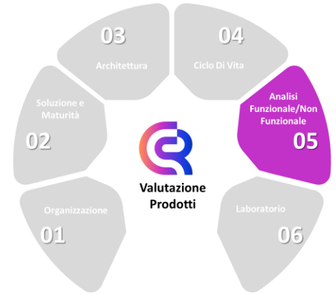
DOCUMENTAZIONE UTENTE

Si verifica la documentazione prodotta è complete ed aggiornata

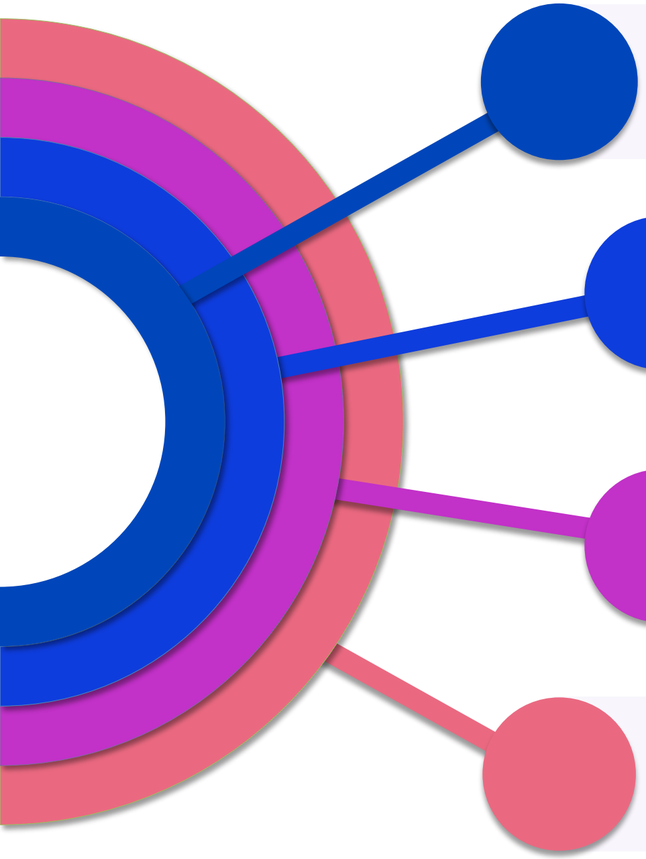
CICLO DI VITA

Si verifica la documentazione inerente l'intero ciclo di vita della soluzione, dalla fase di Progetto al rilascio in esercizio, nonchè eventuali test di sicurezza, etc.

Metodologia CSR – Dominio Analisi Funzionale/Non Funzionale



Si osservano le principali dimensioni di analisi della soluzione (requisiti funzionali, non-Funzionali, etc.)



USABILITÀ/AFFIDABILITA’

Si analizza la capacità del prodotto di essere compreso, appreso, utilizzato e di erogare e mantenere un livello idoneo di prestazioni

MANUTENZIONE/PORTABILITA’

Si verifica la capacità del prodotto di essere modificato, adattato, aggiornato ai contesti e di essere trasferito su diversi ambienti di impiego

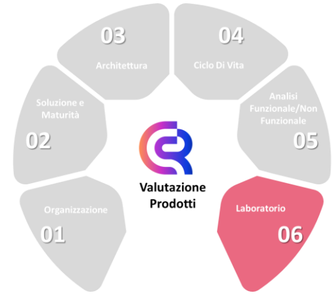
PRESTAZIONI/EFFICACIA

Si verifica la capacità del prodotto di fornire prestazioni in relazione alle risorse impiegate

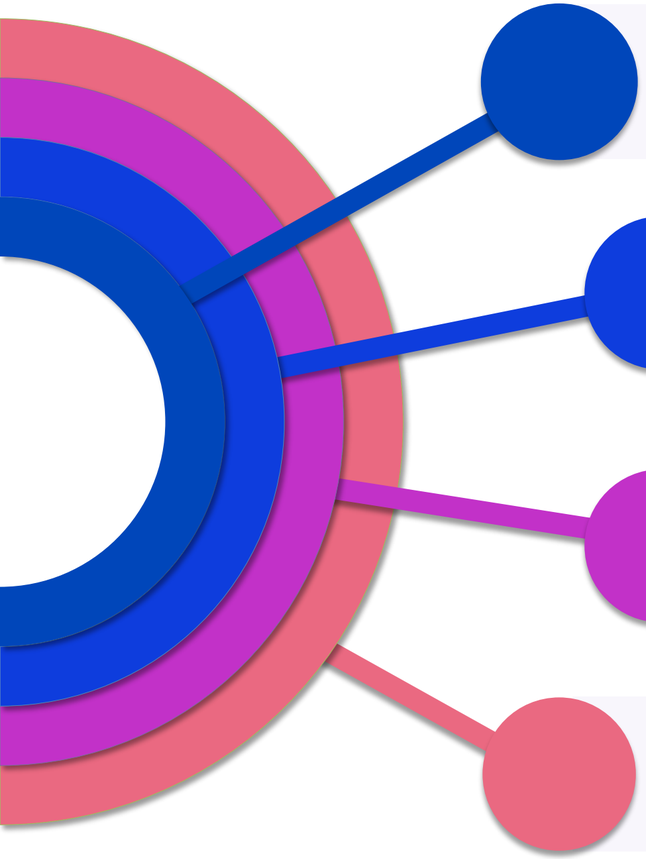
FUR - FUNCTIONAL USER REQUIREMENT

Si verificano le funzionalità, le risposte che l’utente aspetta in determinate condizioni, i risultati che la soluzione/prodotto deve produrre in risposta a specifici input

Metodologia CSR – Dominio Test ed Analisi Laboratorio



Test e Verifiche di Laboratorio tecnologiche sul prodotto e verifiche sulle vulnerabilità



SAST/DAST

Si analizzano i risultati delle attività di Static Application Security Testing (SAST) e Dynamic Application Security Testing (DAST) effettuate

VULNERABILITY ASSESSMENT

Si analizzano i risultati delle attività di Vulnerability Assessmente effettuate

PENETRATION TEST

Si analizzano i risultati delle attività di Penetration Test effettuate

THREAT INTELLIGENCE

Si analizzano i risultati delle attività di Threat Intelligence effettuate,dipendenze con Terze Parti, etc

CYBERSECURITYREADINESS.IT

Grazie per l'attenzione.