SOGEI - Società Generale di Informatica SpA

ing. Fabio LAZZINI, Responsabile Security Governance & Privacy

Cybersecurity per la PA: approccio multicompliance Sogei

ITASEC17 Italian Conference on Cybersecurity – Venezia, 17 gennaio 2017

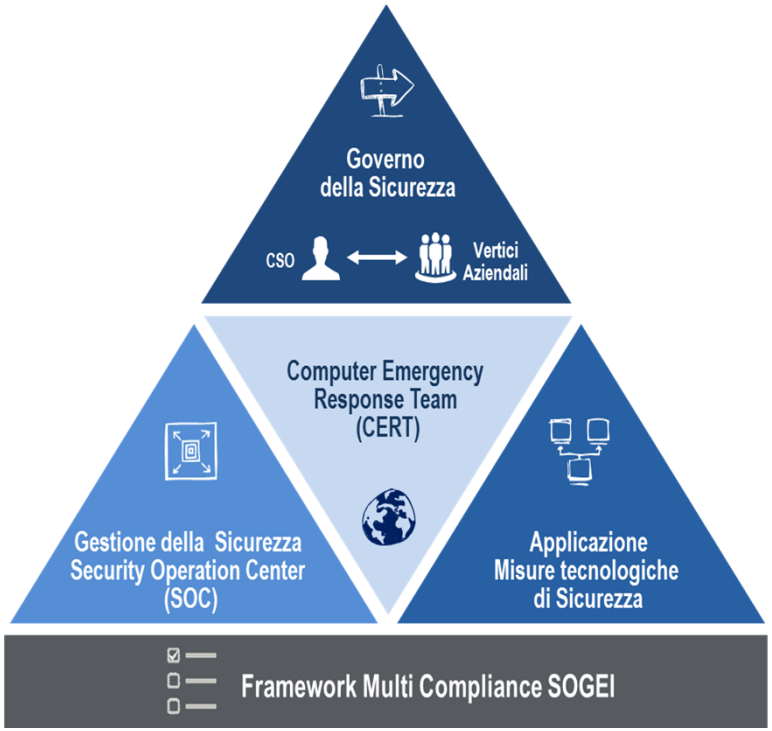
Cybersecurity: punti di attenzione per la PA

Governance complessa	L'**architettura istituzionale a protezione dello spazio cibernetico** rende **complessi** i processi di indirizzo e controllo per la ***cybersecurity*** *nazionale*
Cultura della sicurezza e consapevolezza del rischio cyber	L'affermarsi in modo sempre più consistente di **scenari di rischio** che **compromettono la sicurezza dei servizi offerti** comporta la definizione di percorsi di formazione e **consapevolezza sulla cybersecurity** a ogni livello (**cittadini, operatori e dirigenti della PA**) favorendo l'attuazione di idonei **comportamenti digitali**
Digital transformation vs information security	Il **rapido sviluppo di soluzioni di massa** basato su nuove tecnologie (es. mobile) implica la **continua analisi dei rischi di sicurezza** e la conseguente evoluzione delle misure di protezione con un effort che rende auspicabile la formalizzazione di regole e criteri per la creazione di PPP (Public-Private Partnership)
Information Sharing	Sono **necessari canali di comunicazione definiti, sicuri ed efficaci per la condivisione di informazioni su incidenti in corso, metodi di attacco utilizzati e tecniche di difesa** fra tutti i soggetti governativi pubblici e privati secondo il principio del *need-to-know*
Protezione dei dati personali	Il **nuovo Regolamento europeo per la protezione dei dati personali,** definitivamente applicabile in via diretta in tutti i Paesi UE dal 2018**,** introduce **novità importanti come *data breach* e *privacy impact assessment*** e impone la definizione dei meccanismi di protezione fin dalla progettazione delle attività e per l'intero ciclo di vita dei dati (**privacy by default e security by design**)
Framework comuni contestualizzati	Nonostante l'elevato numero di norme, regolamenti e best practice, **manca un modello integrato di sicurezza che costituisca un unico sistema di riferimento per la PA** consentendo di valutare in modo omogeneo i rischi di sicurezza e di predisporre efficaci programmi per affrontare le minacce cyber.

Cybersecurity: modello di governance Sogei

Le misure per la protezione della sicurezza **fisica** e **logica** sono gestite in modo coordinato in presidi che operano in conformità a normative, regole e standard degli organismi di settore

Il **modello Sogei di Security Governance** è basato su **tre livelli di azione** che consentono di garantire la gestione e il raggiungimento degli obiettivi di protezione definiti anche in considerazione della loro evoluzione



LEADERSHIP E INDIRIZZO

1

- orienta le strategie aziendali verso le tematiche di sicurezza e ne sostiene l'attuazione
- i Vertici sono coinvolti nel governo integrato dell'intera "filiera di sicurezza": cybersecurity, sicurezza delle informazioni e protezione dei dati personali

COORDINAMENTO E CONTROLLO

2

- supervisiona l'attuazione delle misure di sicurezza affinché i requisiti siano effettivamente recepiti dalle strutture preposte allo sviluppo, all'erogazione e alla manutenzione di software, infrastrutture, sistemi e servizi tramite i Sistemi di Gestione della Sicurezza, il SOC e il CERT

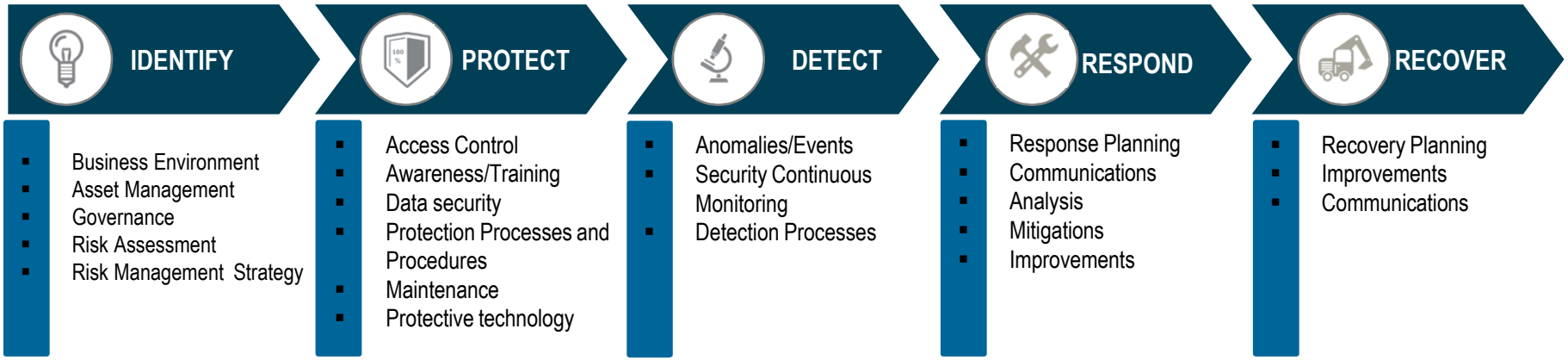
ATTUAZIONE DELLE MISURE DI PROTEZIONE

3

- realizza e gestisce operativamente le misure tecnologiche di sicurezza (protezione delle sedi fisiche e dei data center, protezione delle reti e delle infrastrutture tecnologiche, protezione dei dati e delle informazioni)
- opera in linea con le strategie, gli obiettivi e i criteri definiti

FOURSec: il Framework Multicompliance Sogei per la PA

Framework Nazionale per la Cybersecurity



Framework Multicompliance

Norme

- D. Lgs.196/03
- Provvedimenti Garante
- Misure minime di sicurezza ICT per PA - AgID
- …

Rischi

- Accesso logico non autorizzato
- Vulnerabilità del SW
- Trattamento non consentito di dati personali
- …

Metodologia di Assessment

- Profilo di sicurezza:
  - ✓ conformità
  - ✓ rischio
  - ✓ maturità

Framework MultiCompliance: obiettivi

1. **Creare una vista integrata** della normativa e dei rischi su cybersecurity, sicurezza delle informazioni e privacy fornendo un linguaggio comune

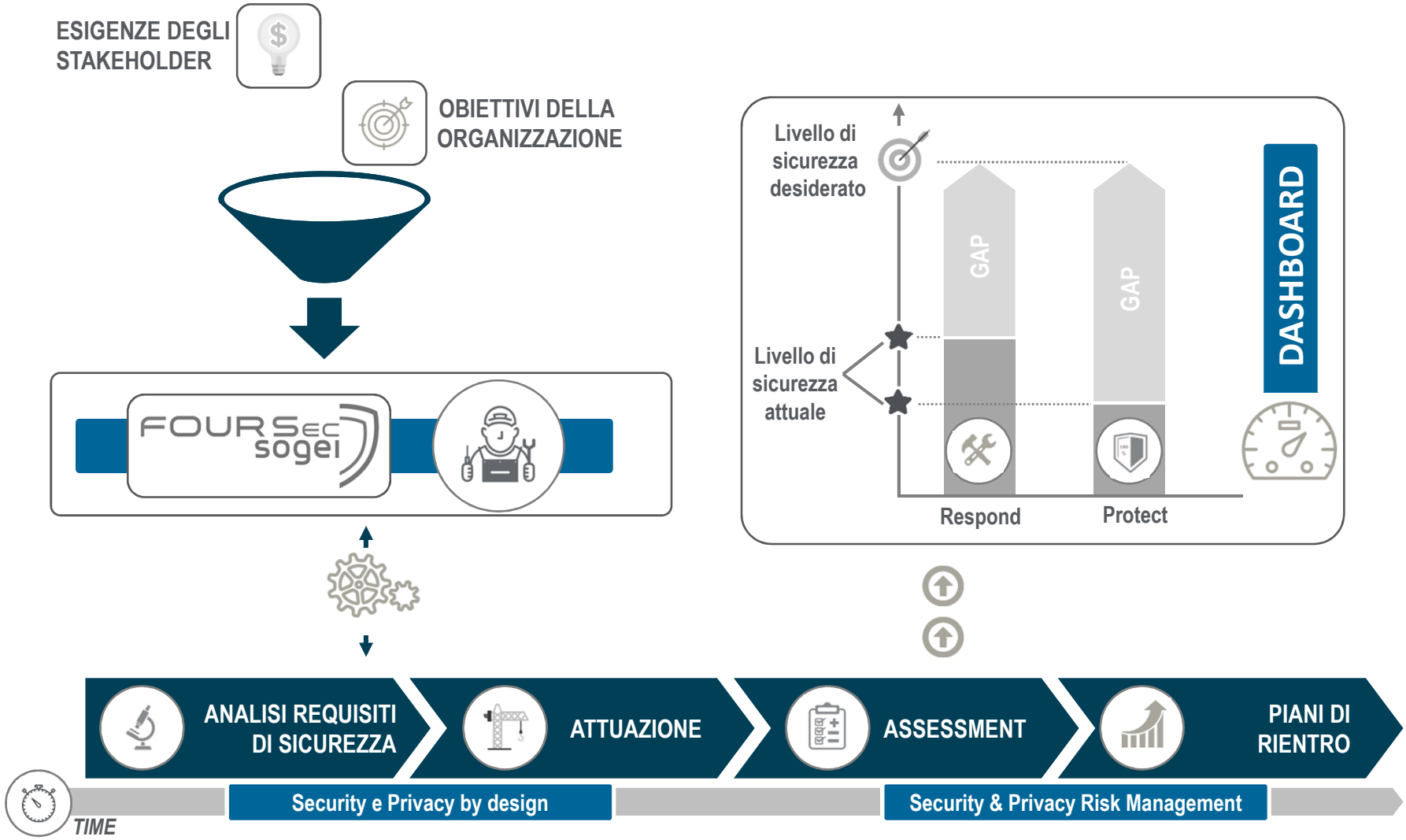
2. Valutare il **livello di sicurezza attuale** dell'**organizzazione** e identificare le **criticità** per specifici **domini (normativo, tecnologico, organizzativo)**

3. **Comunicare** in modo comprensibile e sintetico i **rischi ai Vertici** per identificare le priorità di intervento

4. Definire le **iniziative di miglioramento** e valutare **costi e risorse** necessarie per raggiungere il livello di sicurezza desiderato

5. Offrire un servizio innovativo basato su un **approccio integrato** per valutare i **Rischi** , la **Conformità** e la **Maturità** relativi alla sicurezza delle informazioni

Applicazione del Framework MultiCompliance: design e assessment



Metodologia di assessment: rating

Rating della conformità

Obiettivo: Valutare la conformità delle misure di protezione a quanto previsto da normative e standard di sicurezza.
Metodo: Assegnare il livello di copertura delle misure rispetto ai requisiti di sicurezza.

Rating del rischio

Obiettivo: Individuare gli scenari di rischio e valutarne il livello di rischio corrente (dopo l'applicazione delle misure).
Metodo: Assegnare il grado di robustezza alle misure implementate in relazione alla criticità dei dati trattati ed effettuare un monitoraggio continuo per la rivalutazione dell'efficacia ed efficienza delle misure (CERT, SOC,..).

Rating della maturità

Obiettivo: Valutare il "livello di maturità" dell'organizzazione rispetto alla gestione dei rischi sulla base degli *implementation tier* del *Framework Nazionale for Improving Critical Infrastructure Cybersecurity* (NIST).
Metodo: Assegnare il "livello di maturità" dei processi, dell'infrastruttura e delle persone rispetto ai 4 livelli definiti dal NIST: *Partial, Risk Informed, Repeatable, Adaptive.*

Conclusioni

Sogei ha sviluppato un Framework Multicompliance e un metodo di Cybersecurity Rating che permettono di:

integrare gli aspetti di **cybersecurity** e **sicurezza delle informazioni** con gli adempimenti per la **protezione dei dati personali**

valutare il **profilo corrente** e, ove necessario, definire le iniziative di miglioramento sulla base delle criticità di **conformità normativa, rischio e maturità**

dimostrare agli stakeholder (cittadini, istituzioni, fornitori, clienti) l'**attenzione** posta nella gestione del **rischio cibernetico**

supportare i vertici nell'indirizzare e definire iniziative di miglioramento dei processi di Cybersecurity Risk Management[1] :

- **strategia**, **pianificazione** e **controllo**
- sicurezza come **investimento**
- cooperazione tra **pubblico e privato**
- razionalizzazione del **patrimonio informativo**
- **formazione**

(1) Libro bianco "Il Futuro della Cyber Security in Italia"- CINI

FOR
OUR
SECURITY

FOURSec

sogei

FRAMEWORK TO ORGANIZE UNDER RULES SECURITY

Sede Legale Via M. Carucci n. 99 - 00143 Roma

www.sogei.it