AGID
Agenzia per l'Italia Digitale

FormezPA

FORMAZIONE AGID – FORMEZ SULLA TRANSIZIONE DIGITALE DELLA PA

Progetto Informazione e formazione per la transizione digitale della PA nell'ambito del progetto «Italia Login – la casa del cittadino»

(A valere sul PON Governance e Capacità Istituzionale 2014-2020)

UNIONE EUROPEA
Dipartimento della Funzione Pubblica
PON
AGID Agenzia per l'Italia digitale

AGID
Agenzia per l'Italia Digitale

FormezPA

La sicurezza Informatica nella Pubblica Amministrazione

Strumenti di prevenzione per la sicurezza informatica

02/12/2021

Massimiliano Rossi - CERT- AGID

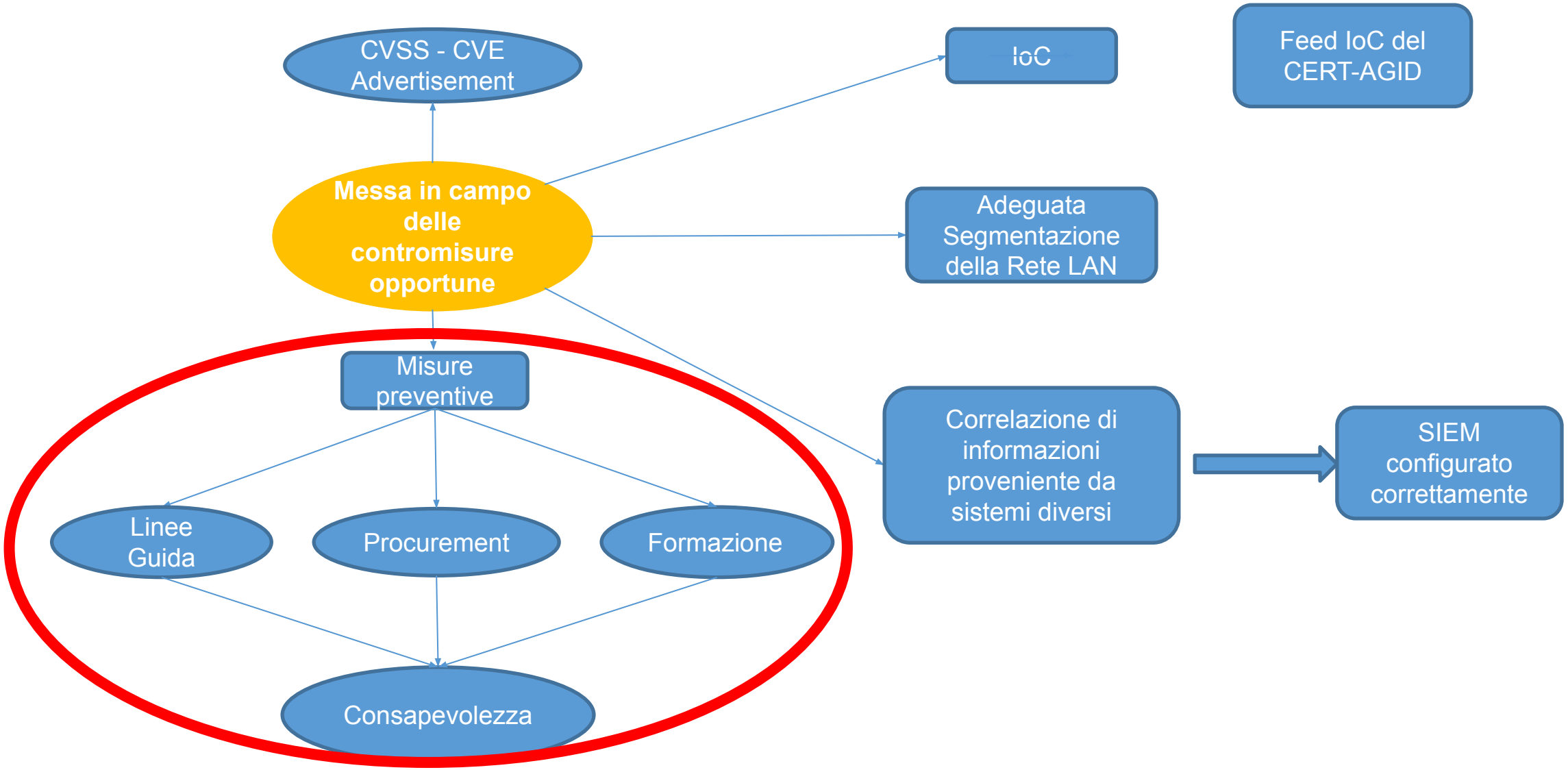
CERT-AGID

UNIONE EUROPEA

Dipartimento della Funzione Pubblica

AGID Agenzia per l'Italia digitale

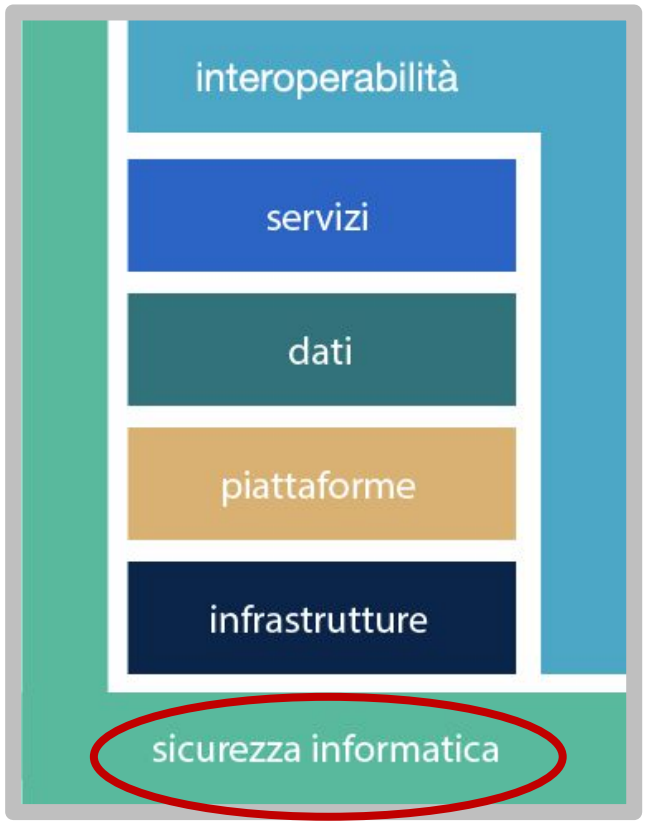
Breve panoramica sulle contromisure/azioni da intraprendere



Contesto di riferimento - la sicurezza informatica delle PA

	INIZIATIVE STRATEGICHE E LINEE GUIDA	SERVIZI E SOLUZIONI OPERATIVE
Ambito PA	❑ Definizione di azioni nel Piano triennale per l'informatica delle PA ❑ Supporta Consip nella definizione dei requisiti di sicurezza per le gare strategiche	❑ Servizi preventivi di sicurezza informatica ❑ Servizi di Cyber Security Awareness ❑ Servizi sussidiari per la gestione della sicurezza
Ambito generale	❑ Emanazione di Linee Guida ❑ Vigilanza sui Trusted Services	❑ Early warning tramite avvisi e bollettini di sicurezza ❑ Infosec con statistiche e dati analitici su Pattern di attacco, Vulnerabilità e IoC ❑ Tool di Cyber Risk Assessment

Il Piano triennale per l'informatica nella PA 2020-2022



IMPOSTAZIONE DEL PIANO

- **Semplificazione** della struttura del documento e dei capitoli
- Particolare rilevanza per **le azioni specifiche** da porre in essere da parte delle PA

Circa **100 azioni nel triennio a carico delle PA** con focus e indicazioni specifiche sulle azioni delle **PA**

EFFICACIA DEL PIANO

- Valorizzazione della trasversalità delle componenti interoperabilità **e sicurezza informatica**
- Evidenziazione degli **aspetti organizzativi** necessari al completamento del percorso di trasformazione digitale delle PA

MONITORAGGIO DEL PIANO

- Introduzione di un approccio orientato alla misurazione dei risultati
- Individuazione di un percorso operativo che coinvolga le PA nell'attività di monitoraggio del Piano

La sicurezza nel Piano triennale 2020 – 2022

L' esigenza per la PA di contrastare le minacce cibernetiche è fondamentale in quanto garantisce non solo la disponibilità, l'integrità e la riservatezza delle informazioni proprie del Sistema informativo della Pubblica Amministrazione, ma è il presupposto per la protezione del dato che ha come conseguenza diretta l'aumento della fiducia nei servizi digitali erogati dalla PA.

OBIETTIVI DEL Cap. 6

1. Aumentare la **consapevolezza del rischio cyber** (Cyber Security Awareness) nelle PA

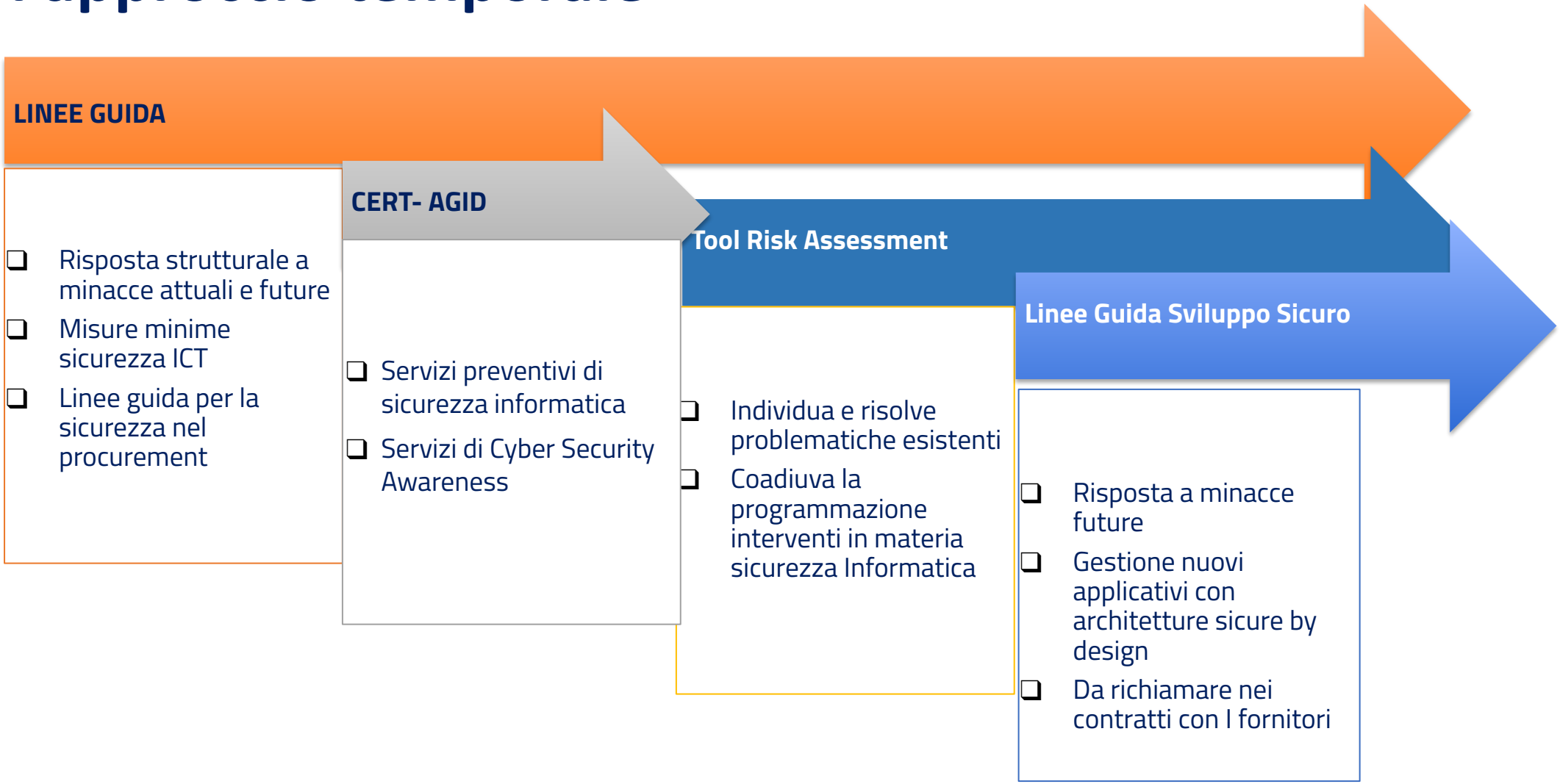
2. Aumentare il livello di **sicurezza informatica dei portali istituzionali** della Pubblica Amministrazione

RISULTATI ATTESI

- ❑ Incremento del livello di Cyber Security Awareness nella PA

- ❑ Incremento del numero dei portali istituzionali che utilizzano il protocollo HTTPS only
- ❑ Massimizzazione del numero dei Content Management System (CMS) non vulnerabili utilizzati nei portali istituzionali delle PA

Azioni e strumenti integrati di prevenzione - l'approccio temporale



Sicurezza: Il ruolo e gli strumenti per le PA

AgID opera per mantenere e sviluppare servizi di sicurezza preventivi e funzioni di accompagnamento utili per la crescita e la diffusione della cultura della sicurezza informatica, in linea con le disposizioni del CAD e con gli obiettivi descritti dal Piano triennale per l'informatica nella pubblica amministrazione

- Servizi e strumenti di sicurezza preventivi
- Funzioni di accompagnamento

STRUMENTI

- ❑ Risk Assessment Tool per le PA
- ❑ Linee Guida
- ❑ Piattaforma Infosec
- ❑ Trasmissione automatizzata IoC
- ❑ Strumento di autoverifica HTTPS e CMS per le PA

→ **Cyber Security dei servizi digitali offerti dalle PA e non solo...**

Linee di indirizzo e linee guida AGID sulla sicurezza Informatica

Linee per la sicurezza nel procurement ICT

Le linee guida contengono indicazioni sulle misure di sicurezza che le PA devono adottare per garantire la sicurezza nel processo di acquisto di beni e servizi ICT

Linee per lo sviluppo del software sicuro

Le linee guida contengono indicazioni per garantire un ciclo di sviluppo di software sicuro all'interno delle amministrazioni

Misure minime di sicurezza ICT

Adottate da AGID nel 2017 contengono indicazioni di natura tecnologica, organizzativa e procedurale utili alle Amministrazioni per valutare il proprio livello di sicurezza informatica

Raccomandazioni AGID - TLS e Cipher Suite

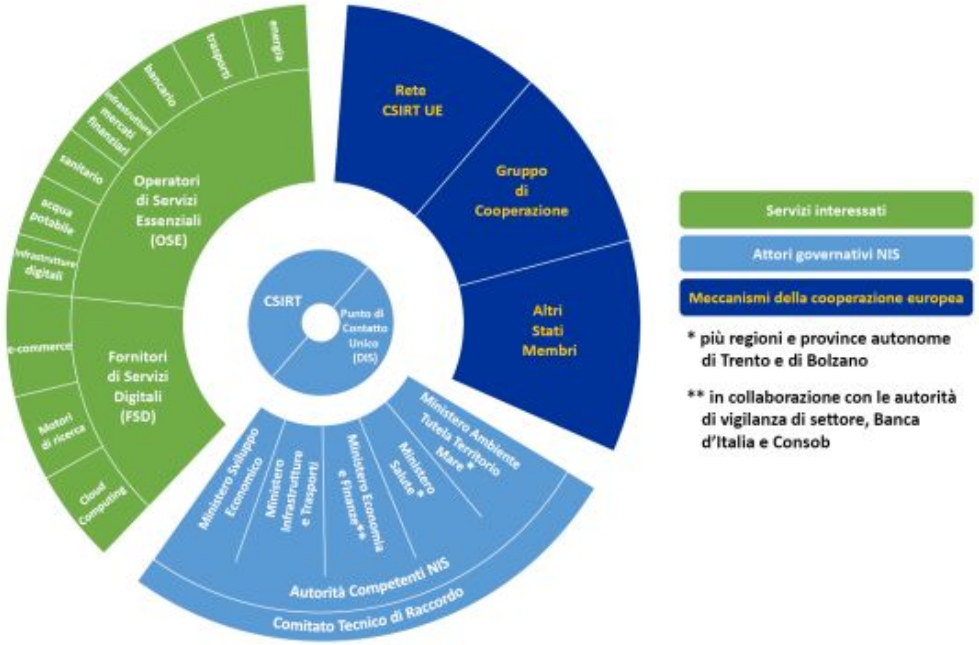
Il documento, redatto di concerto con il MiD / Dipartimento per la trasformazione digitale, fornisce un insieme di raccomandazioni in merito ai protocolli di sicurezza e alle Cipher Suite

Informazioni utili…

Con il Decreto Legislativo 18 maggio 2018, n.65, pubblicato sulla Gazzetta Ufficiale n. 132 del 9 giugno 2018, l'Italia ha dato attuazione, recependola nell'ordinamento nazionale, alla Direttiva (UE) 2016/1148, cd. Direttiva NIS, intesa a definire le misure necessarie a conseguire un elevato livello di sicurezza delle reti e dei sistemi informativi. Il decreto si applica agli Operatori di Servizi Essenziali (OSE) e ai Fornitori di Servizi Digitali (FSD).

Gli **OSE** sono i soggetti, pubblici o privati, che forniscono servizi essenziali per la società e l'economia nei settori sanitario, dell'energia, dei trasporti, bancario, delle infrastrutture dei mercati finanziari, della fornitura e distribuzione di acqua potabile e delle infrastrutture digitali.

Gli **FSD** sono le persone giuridiche che forniscono servizi di e-commerce, cloud computing o motori di ricerca, con stabilimento principale, sede sociale o rappresentante designato sul territorio nazionale.



https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2018/06/La-NIS-in-pillole.pdf

Sia gli OSE che gli FSD:

- sono chiamati ad adottare misure tecniche e organizzative adeguate e proporzionate alla gestione dei rischi e a prevenire e minimizzare l'impatto degli incidenti a carico della sicurezza delle reti e dei sistemi informativi, al fine di assicurare la continuità del servizio;
- hanno l'obbligo di notificare, senza ingiustificato ritardo, gli incidenti che hanno un impatto rilevante, rispettivamente sulla continuità e sulla fornitura del servizio, al Computer Security Incident Response Team (CSIRT) italiano, informandone anche l'Autorità competente NIS di riferimento.

Altre informazioni utili….

GDPR

Notifica all'autorità di controllo

- In che tempi? Senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui il titolare del trattamento è a conoscenza del data breach
- Art. 32 – Princio dell'accountability

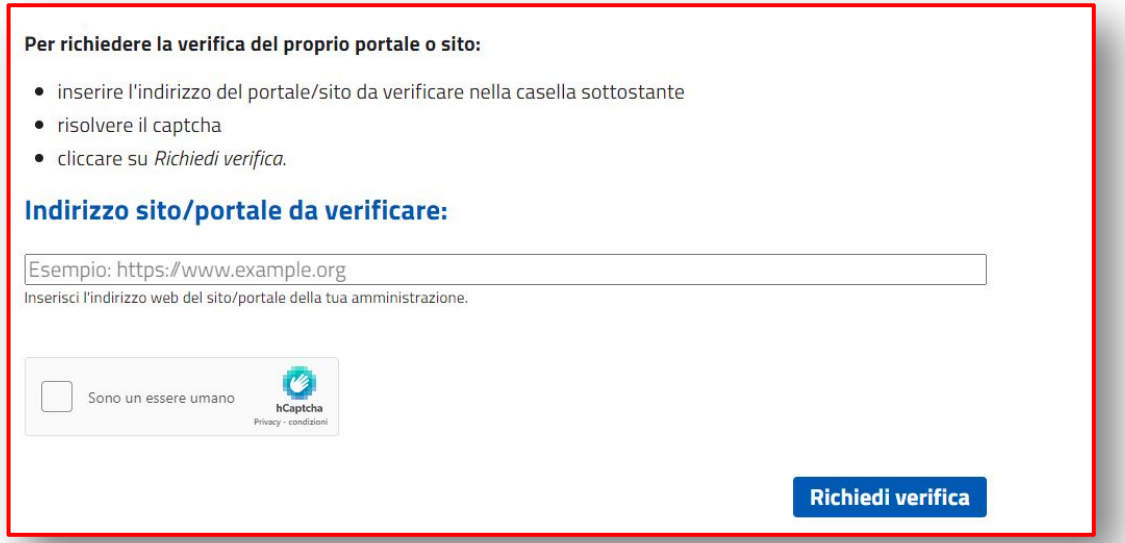
Responsabile della Transizione al digitale

Coordinamento strategico dello sviluppo dei sistemi informativi. Art.17 del CAD

Sicurezza: strumento di autoverifica per le PA

Servizio di autoverifica della configurazione HTTPS e CMS dedicato alle PA

Questo servizio consente alle Amministrazioni di richiedere un **report** contenente la verifica della configurazione HTTPS e dello stato di aggiornamento del CMS, se presente e rilevabile, del portale/sito **indicato nella propria scheda IPA**.



Condivisione di indicatori di compromissione per la protezione della Pubblica Amministrazione

Le Pubbliche Amministrazioni interessate possono esprimere la volontà di aderire al flusso di Indicatori di compromissione (**Feed IoC**) del **CERT-AGID** per la protezione della propria Amministrazione da minacce Malware e Phishing compilando l'apposito modulo.

Come aderire

1. Scarica e compila il modulo di accreditamento in formato Libre Office o in formato Microsoft Office.
2. Compila il modulo con i riferimenti della persona tecnica e l'elenco (max 20) di indirizzi IPv4 da abilitare.
3. Invia il modulo compilato per e-mail a **info@cert-agid.gov.it.**

Per maggiori informazioni: https://cert-agid.gov.it/scarica-il-modulo-accreditamento-feed-ioc/

Tool di Cyber Risk Management - Quadro d'insieme

Il tool nasce per supportate le PA nel self-assessment di sicurezza informatica e migliorare la consapevolezza sulle materie di Cyber Security e permette di valutare le vulnerabilità e il livello di esposizione al rischio
Il tool è *web based* e l'accesso per le PA avviene attraverso SPID.

COME FUNZIONA IL TOOL?

FASE INIZIALE

Definizione del contesto in cui opera la PA

FASE DI ANALISI

- ❑ Identificazione dei rischi
- ❑ Simulazione degli effetti di mitigazione delle azioni
- ❑ Piano dei trattamenti

FASE OPERATIVA

VALUTAZIONE DELLE AZIONI DA METTERE IN CAMPO Orizzontale su tutta la PA o su singoli servizi

UNIONE EUROPEA
Fondo sociale europeo
Fondo Europeo di Sviluppo Regionale

Agenzia per la Coesione Territoriale

Dipartimento della Funzione Pubblica

PON GOVERNANCE E CAPACITÀ ISTITUZIONALE 2014-2020

Metodologia di cybersecurity risk management 1/2

Lo standard di riferimento

ISO 31000: GESTIONE DEL RISCHIO - PRINCIPI E LINEE GUIDA
Standard che fornisce una serie completa di principi e linee guida per aiutare le organizzazioni ad eseguire l'analisi e la valutazione dei rischi.

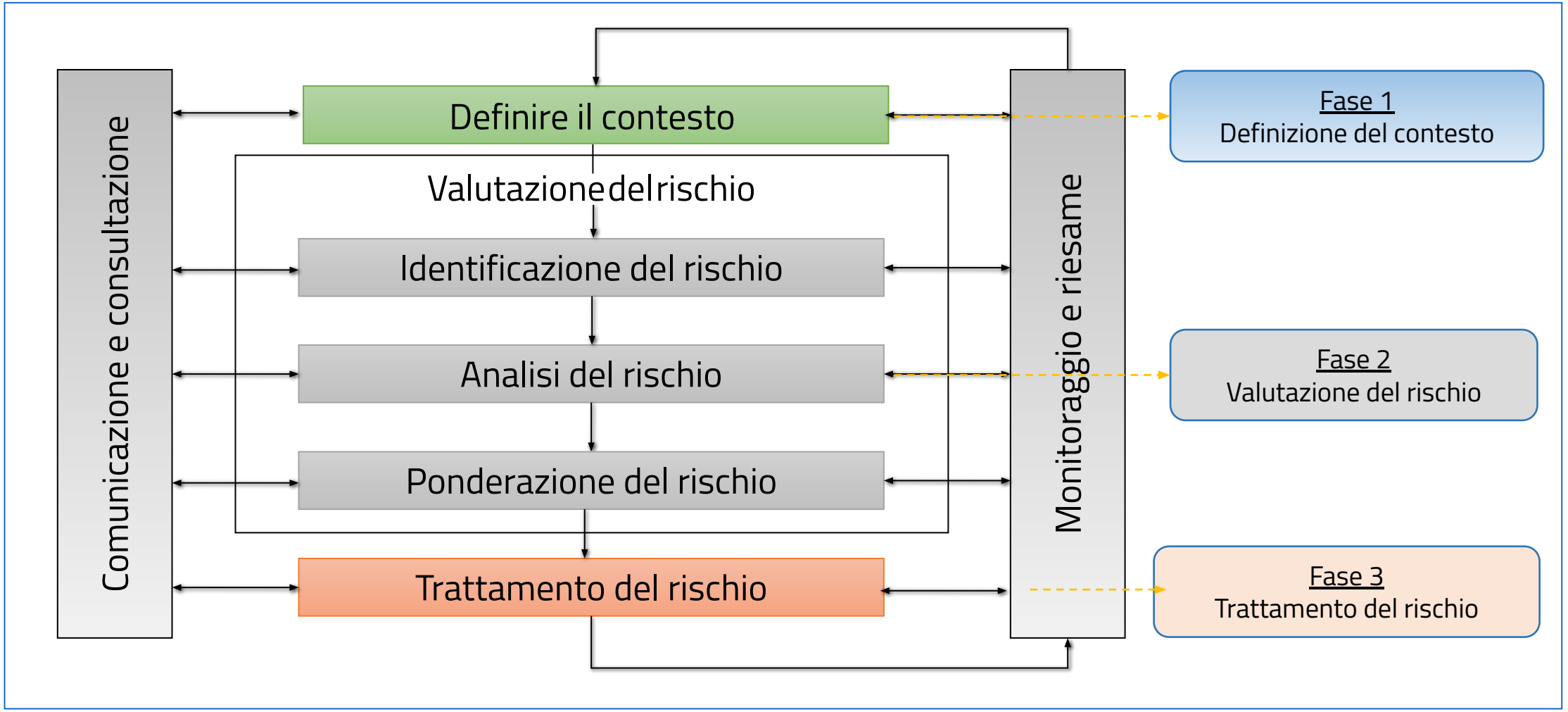
IRAM 2 (ISF): METODOLOGIA DI SECURITY RISK ASSESSMENT
Metodologia di valutazione dei rischi mediante analisi e valutazione di minacce, vulnerabilità e impatti

ISO 27001: SISTEMA DI GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI
Standard utilizzato per arricchire il framework di controlli in ambito information security

NIST
Insieme di pubblicazioni utilizzate per arricchire il framework di controlli in ambito information security

MISURE MINIME DI SICUREZZA ICT PER LE PA
Misure per valutare e migliorare il livello di sicurezza informatica della PA, al fine di contrastare le minacce informatiche più frequenti

Metodologia di cybersecurity risk management 2/2



Macro-modello di calcolo del rischio

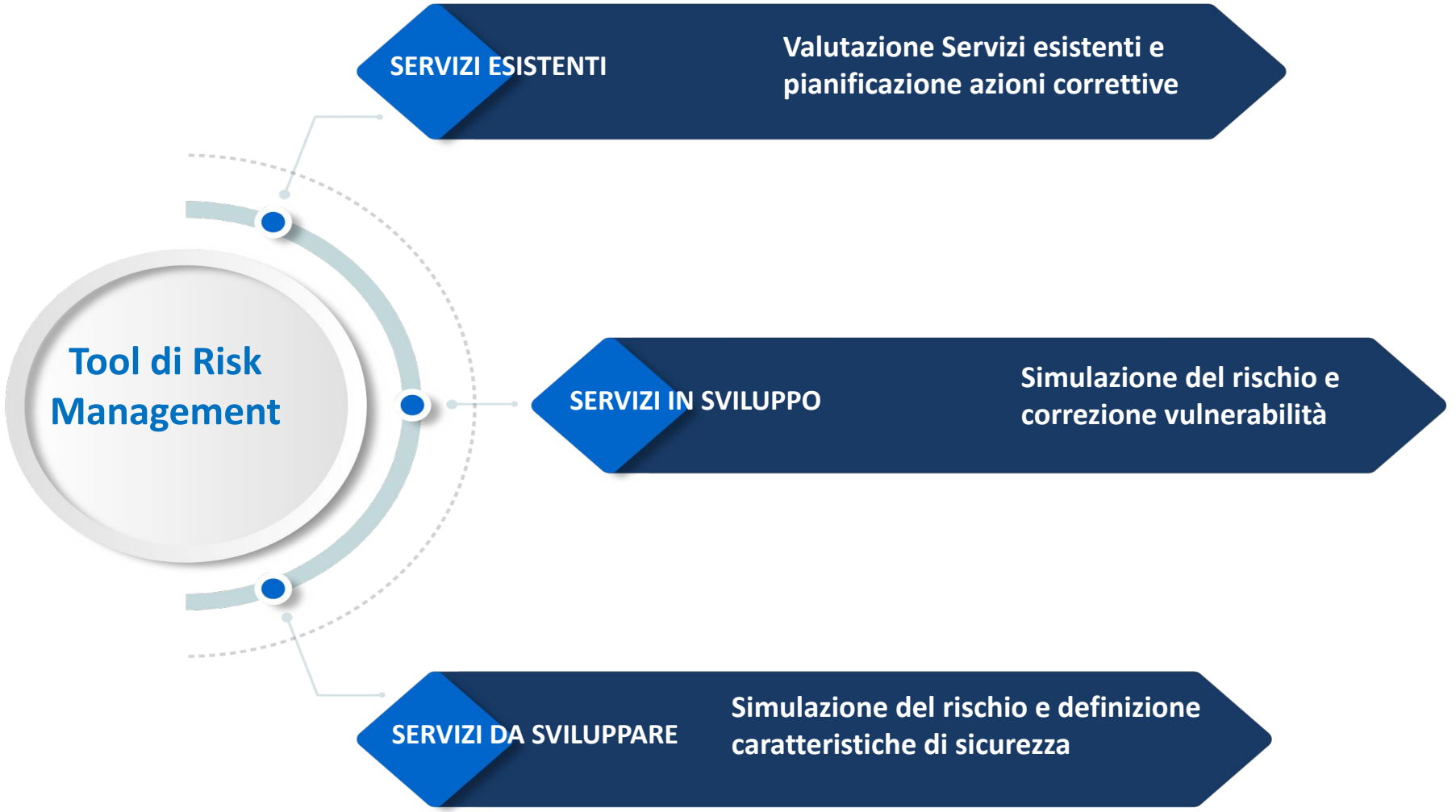
CARATTERISTICHE SERVIZI
A seconda delle caratteristiche primarie dei servizi erogati, è determinato il livello di criticità intrinseca (Profilo di Criticità) della PA. Le caratteristiche primarie e secondarie consentono di selezionare le Misure di Sicurezza da implementare (controlli di tipo amministrativo, sicurezza logica e fisica,) e dunque determinare le Vulnerabilità.

BENCHMARK
Il benchmark consente di valutare il fattore di Esposizione alla singola minaccia per il settore Pubblica Amministrazione.

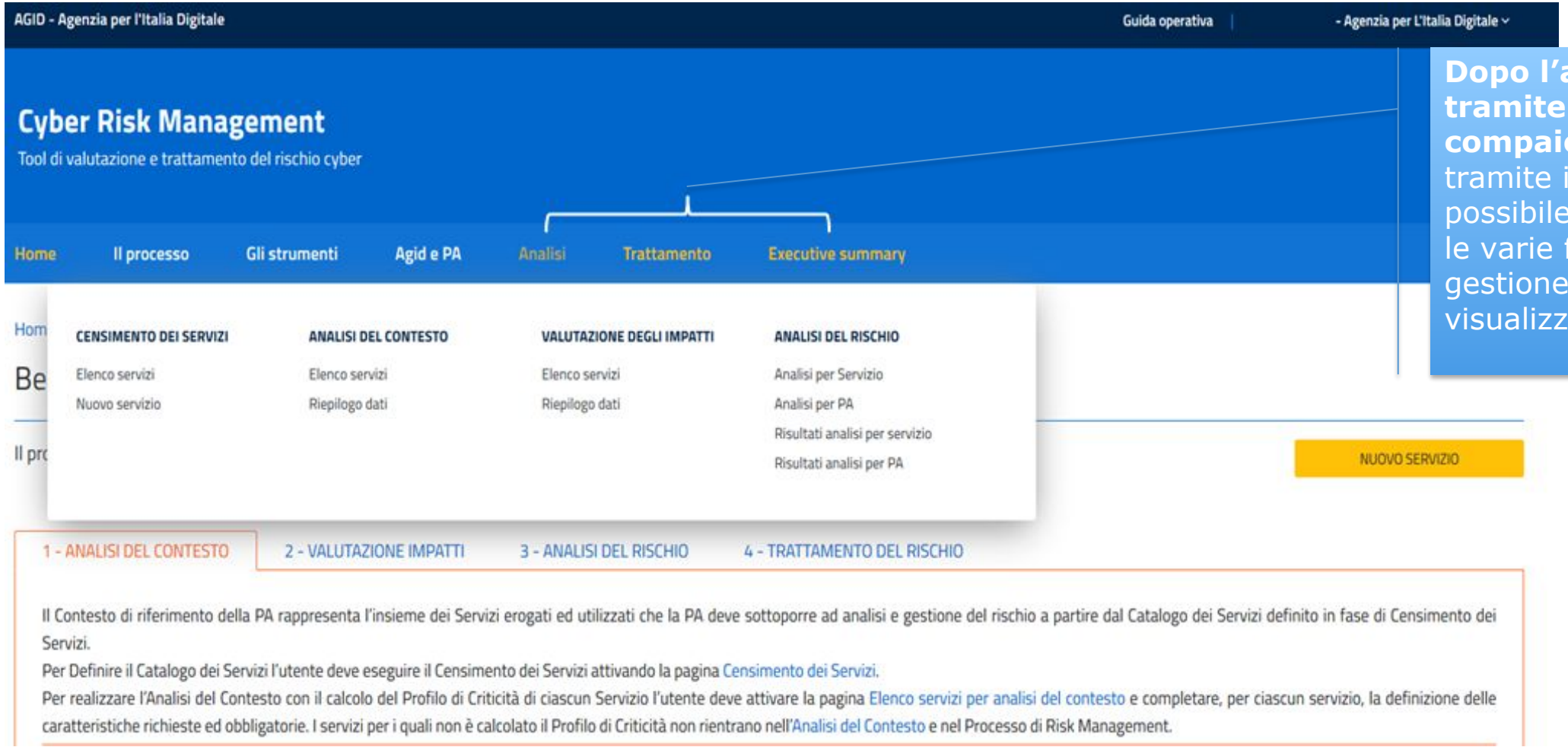
IMPATTO
Consente di valutare gli impatti per ciascun servizio erogato dalla PA in caso di perdita di **Riservatezza (R), Integrità (I) e Disponibilità (D).** A partire dagli impatti sui singoli servizi erogati dalla PA, sarà poi calcolato l'impatto R,I,D sulla PA.

Ambiti di applicazione

Feedback dagli Enti



All’interno del tool di risk assessment

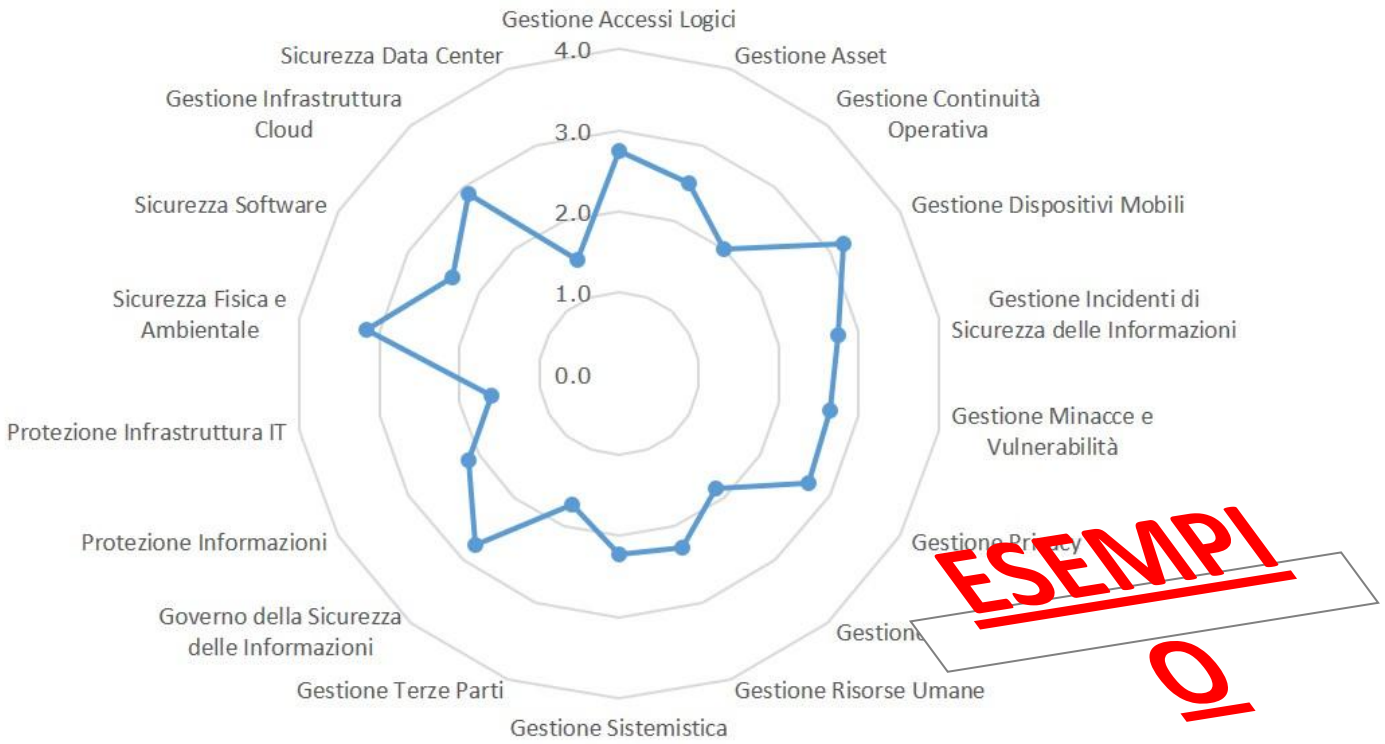


Dopo l’accesso tramite SPID, compaiono tre menù tramite i quali è possibile implementare le varie fasi della gestione del rischio e visualizzarne i risultati.

Esempio di report - risultati analisi del rischio 1/3

Per ciascuna categoria di controlli (dominio di sicurezza) sono riportati i relativi livelli di copertura in base ai risultati dell'assessment:

Grado di implementazione medio per ciascun dominio di sicurezza



Esempio di report - risultati analisi del rischio 2/3

Per ciascuna categoria di minacce sono riportati i relativi livelli di rischio in base ai risultati dell'assessment:

Esempio di report risultati analisi del rischio 3/3

Per ciascuna categoria di minacce sono riportati i relativi livelli di rischio in base ai risultati dell'assessment:

ESEMPIO

Report dei rischi per categoria di minaccia

Attacchi Logici e/o Fisici

Attacchi al sistema di autenticazione

Minaccia	Impatto R-I-D	Vulnerabilità	Esposizione alla minaccia	Probabilità di accadimento	Rischio attuale	Propensione al rischio	Opzioni di trattamento	Rischio derivato
Accesso non autorizzato a credenziali di autenticazione valide	ALTO	ALTO	ALTO	ALTO	ALTO	MEDIO	MITIGARE	ALTO
Session hijacking	ALTO	ALTO	CRITICO	CRITICO	CRITICO	MEDIO	MITIGARE	CRITICO
Sfruttare vulnerabilità nei meccanismi di autenticazione	ALTO	ALTO	CRITICO	CRITICO	CRITICO	MEDIO	MITIGARE	CRITICO

Output Fase:
RISK ASSESSMENT

Output Fase:
RISK MANAGEMENT

Monitoraggio continuo del piano dei trattamenti 1/2

Contatti utili del CERT-AGID:

e-mail : info@cert-agid.gov.it
web : https://cert-agid.gov.it
twitter : @agidcert
telegram : @certagid

Per segnalarci nuove campagne **malware / phishing / scam** da analizzare basta allegare l'email originale sospetta e inviarla all'indirizzo:

malware@cert-agid.gov.it

Grazie per l’attenzione

Massimiliano Rossi

www.agid.gov.it

Riferimenti dei docenti (facoltativi)
Altri riferimenti ritenuti necessari (facoltativi)