AGID | Agenzia per l'Italia Digitale

FormezPA

Strumenti di prevenzione per la sicurezza informatica

Massimiliano Rossi

AgID

25/06/2021

UNIONE EUROPEA
Fondo sociale europeo
Fondo Europeo di Sviluppo Regionale

Agenzia per la Coesione Territoriale

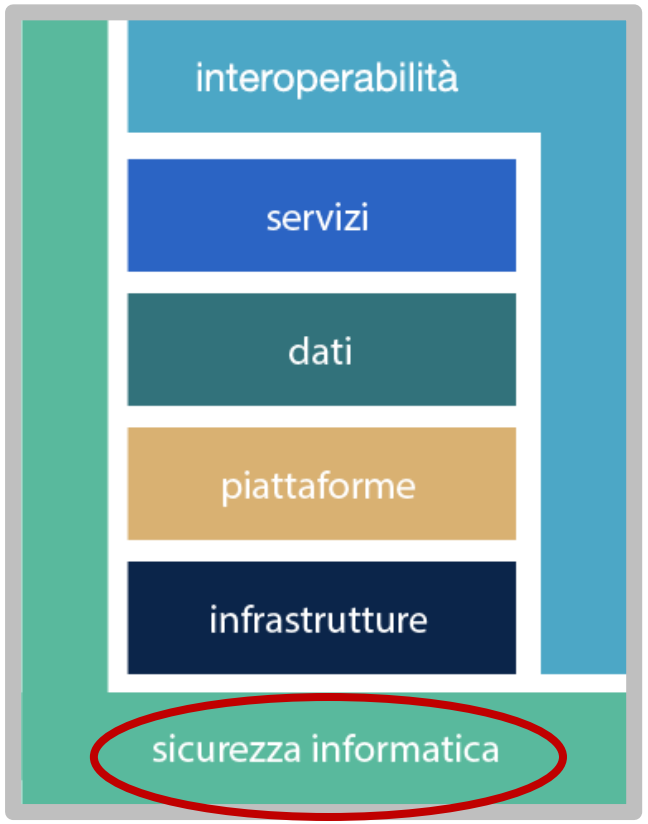
Presidenza del Consiglio dei Ministri
Dipartimento della Funzione Pubblica

PON GOVERNANCE E CAPACITÀ ISTITUZIONALE 2014-2020

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

LINEE GUIDA

- Risposta strutturale a minacce attuali e future
- Misure minime sicurezza ICT
- Linee guida per la sicurezza nel procurement

CERT- AGID

- Servizi preventivi di sicurezza informatica
- Servizi di Cyber Security Awareness

Tool Risk Assessment

- Individua e risolve problematiche esistenti
- Coadiuva la programmazione interventi in materia sicurezza Informatica

Linee Guida Sviluppo Sicuro

- Risposta a minacce future
- Gestione nuovi applicativi con architetture sicure by design
- Da richiamare nei contratti con I fornitori

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

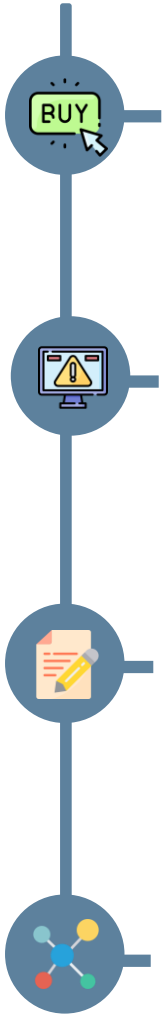
- Servizi e strumenti di sicurezza preventivi
- Funzioni di accompagnamento

STRUMENTI

- ❑ Risk Assessment Tool per le PA
- ❑ Linee Guida
- ❑ Piattaforma Infosec
- ❑ Trasmissione automatizzata IoC

→ **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

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

Presidenza del Consiglio dei Ministri
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.

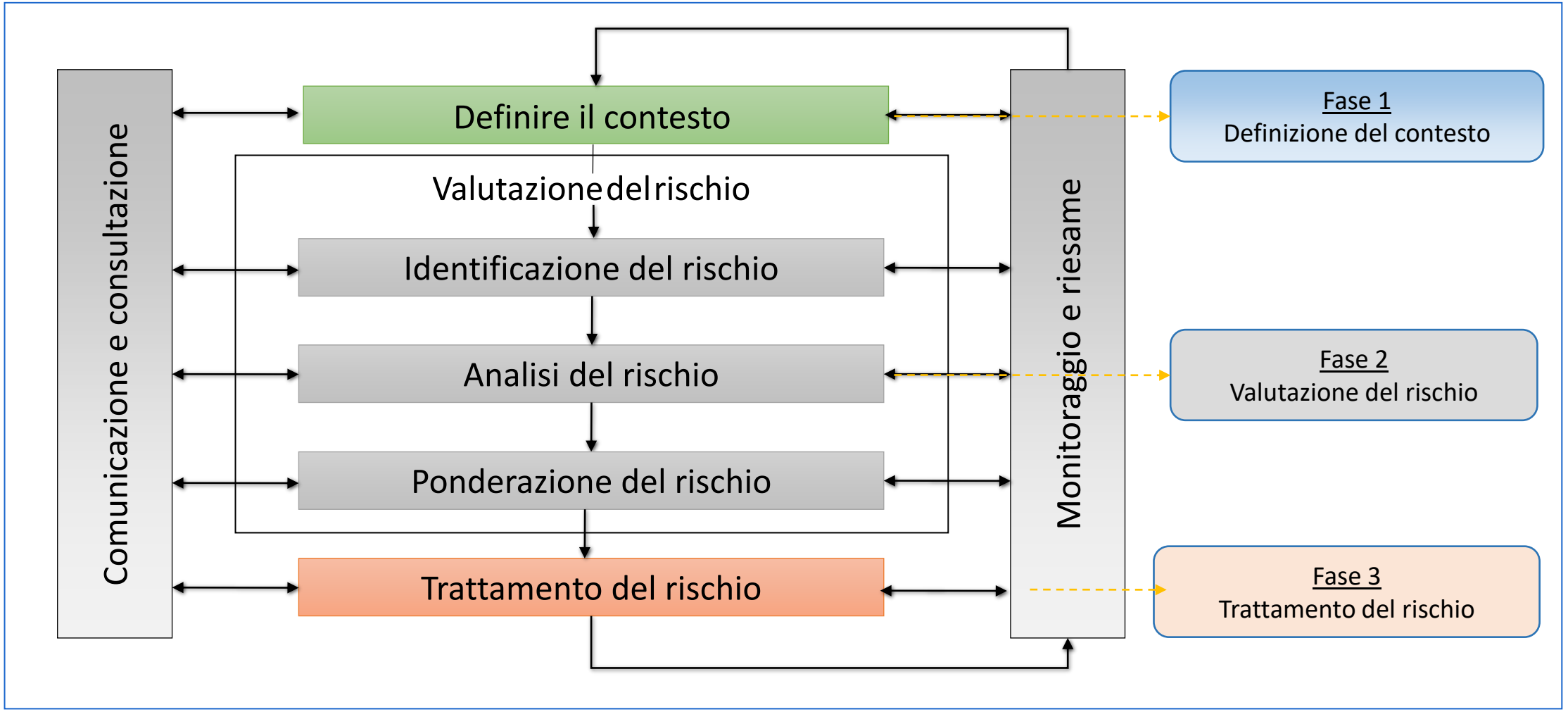
IRAM 2 (ISF): METODOLOGIA DI SECURITY RISK ASSESSMENT
Metodologia di valutazione dei rischi mediante analisi e valutazione di minacce, vulnerabilità e impatti

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 1/2

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.

VULNERABILITÀ

BENCHMARK

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

LIVELLO DI ESPOSIZIONE ALLA MINACCIA

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.

IMPA

Macro-modello di calcolo del rischio 2/2

- Censimento dei servizi oggetto di analisi del rischio.
- Identificazione delle caratteristiche primarie e secondarie di ciascun servizio.
- Calcolo del Profilo di Criticità associato ad ogni servizio.
- Calcolo del Profilo di criticità associato alla PA in funzione dei profili di criticità dei servizi.

RISULTATI

- Per ciascun servizio, valutazione dell'impatto in termini di Riservatezza (R), Integrità (I) e Disponibilità (D) delle informazioni trattate dai servizi per ciascuna categoria di impatto: Economico/Finanziario, Operativo, Reputazionale e Legale/Compliance.
- Valutazione dell'impatto R,I,D della PA in funzione degli impatti sulle singole componenti R-I-D dei servizi.

RISULTATI

- Compilazione del questionario di Risk Assessment per la PA al fine di valutare il livello di vulnerabilità dei vari domini di sicurezza (accessi logici, sicurezza SW, gestione privacy, etc).
- Implementazione di un Risk Assessment report per la PA con indicazione delle componenti di rischio risultanti per ciascuna delle 32 minacce e relative opzioni di trattamento. Posizionamento della PA

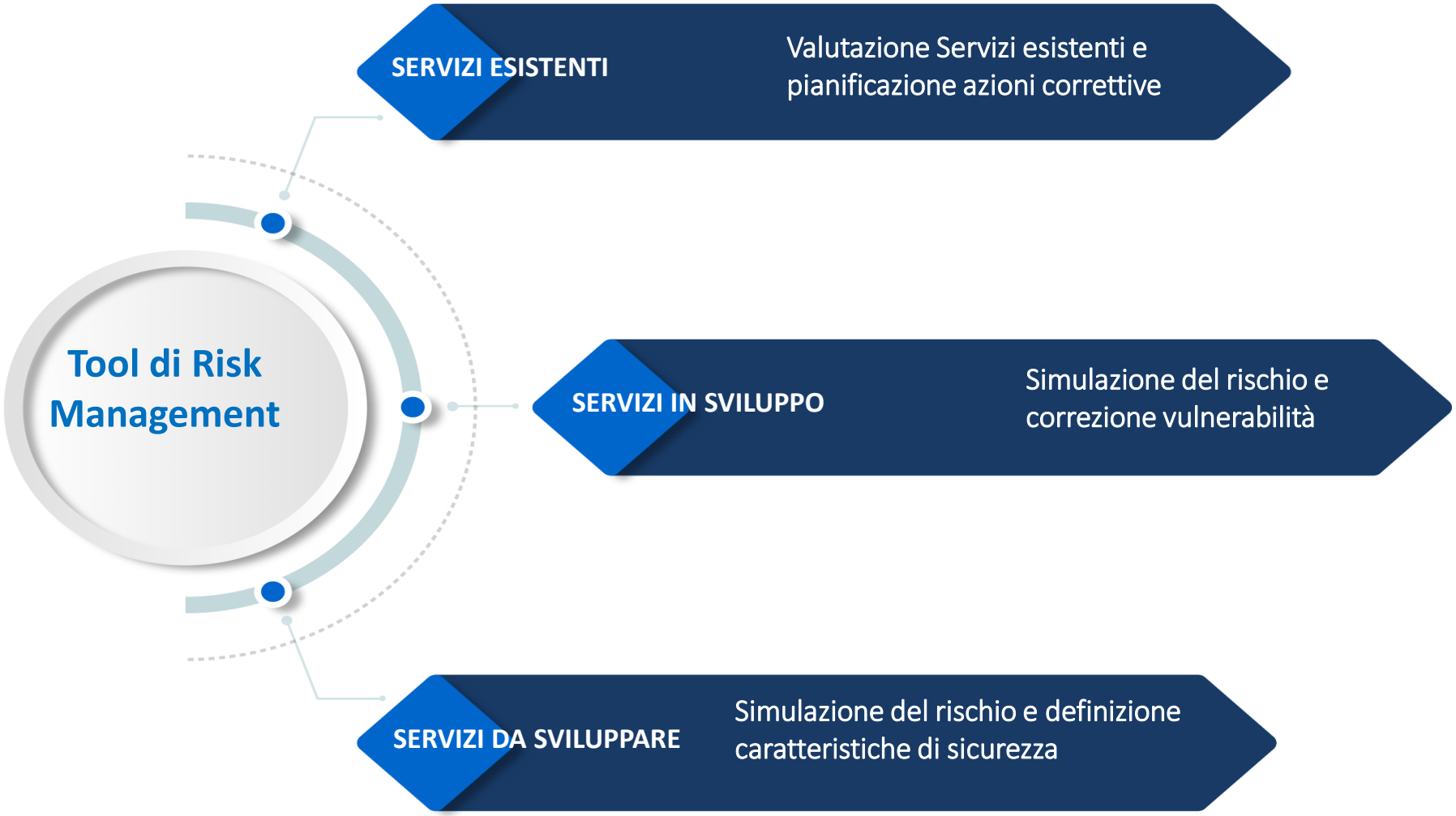
REPORT

- Valutazione dei principali findings emersi dall'analisi del rischio.
- Definizione delle azioni di trattamento e mapping con le convenzioni attive.
- Implementazione di una matrice di prioritizzazione delle azioni di trattamento.
- Valutazione del Rischio Residuo.
- Definizione del Piano di Trattamento del Rischio

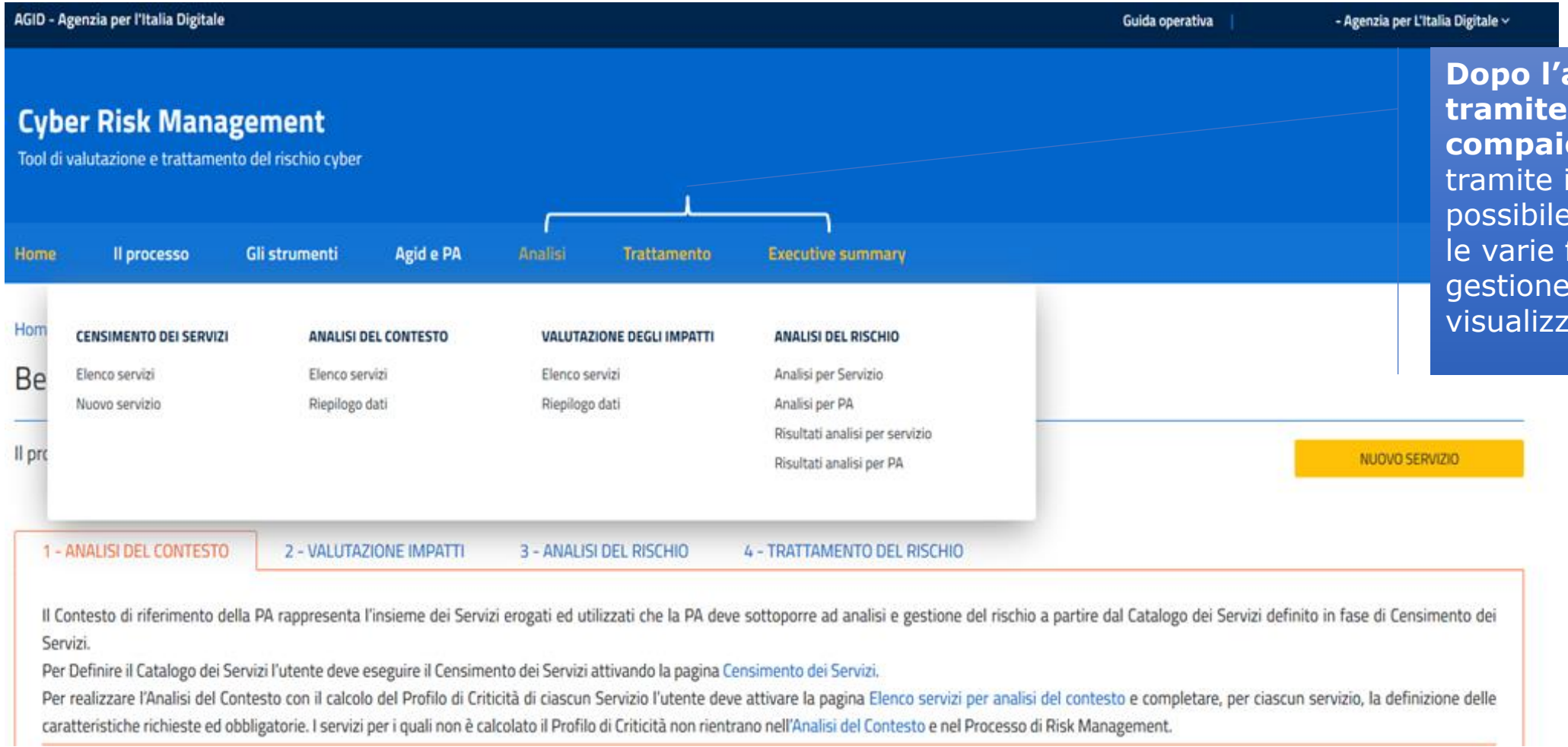
PIANO DI TRATTAMENTO

Ambiti di applicazione

Feedback dagli Enti



All’interno del tool di risk assessment

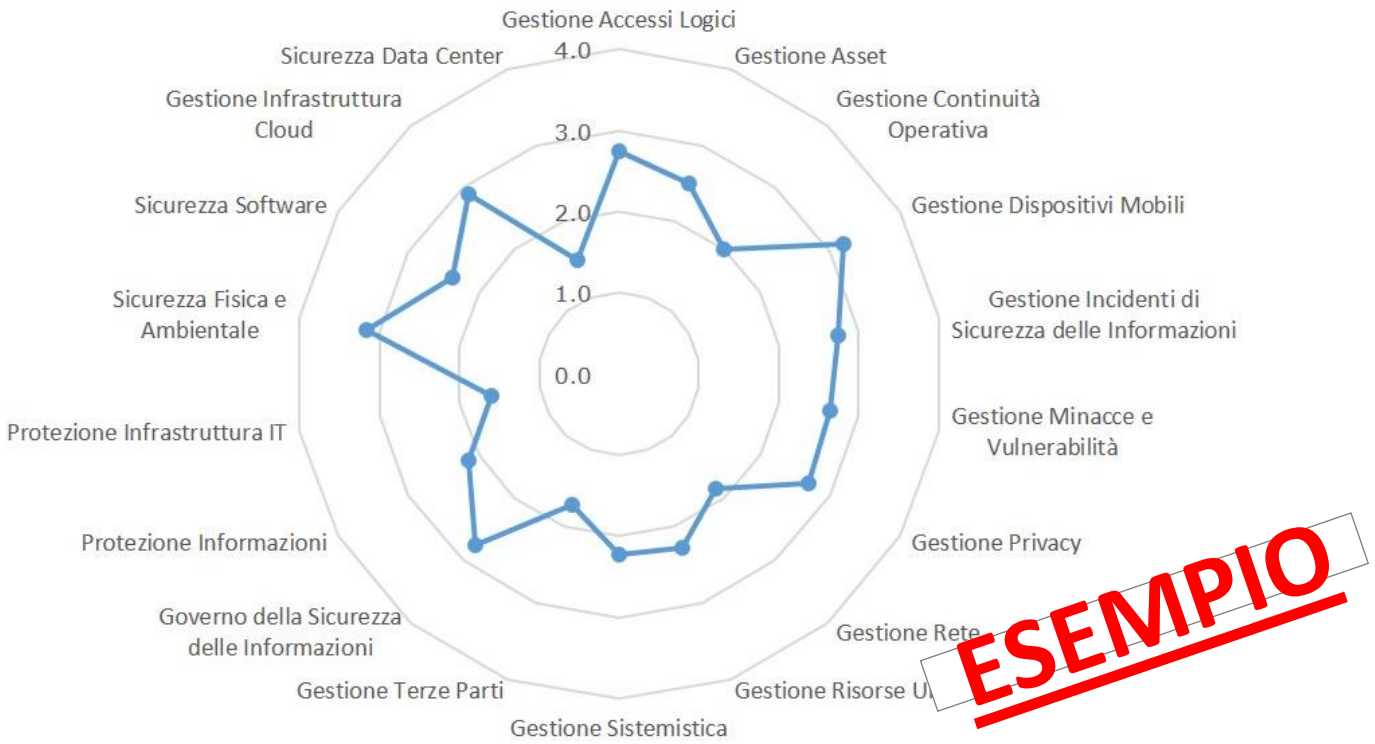


Dopo l’accesso tramite SPID, compaiono tre menù tramite i quali è possibile implementare le varie fasi della gestione del rischio e visualizzarne i risultati.

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:

Distribuzione risposte per dominio di sicurezza

Gestione Accessi Logici
Gestione Asset
Gestione Continuità Operativa
Gestione Dispositivi Mobili
Gestione Incidenti di Sicurezza delle Informazioni
Gestione Infrastruttura Cloud
Gestione Minacce e Vulnerabilità
Gestione Privacy
Gestione Rete

Report dei rischi per categoria di minaccia

Attacchi Logici e/o Fisici
Minacce Ambientali
Minacce Legali
Utilizzo improprio e/o errori

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		MITIGARE	CRITICO
Sfruttare vulnerabilità nei meccanismi di autenticazione	ALTO	ALTO	CRITICO	CRITICO			MITIGARE	CRITICO

ESEMPIO

Attacchi al sistema di comunicazione

Attacchi fisici

Minaccia	Impatto R-I-D	Vulnerabilità	Esposizione alla minaccia	Probabilità di accadimento	Rischio attuale	Propensione al rischio	Opzioni di trattamento	Rischio derivato
Attacchi all'infrastruttura fisica dell'organizzazione	ALTO	ALTO	MEDIO	BASSO	BASSO	MEDIO	ACCETTARE	BASSO
Furto o perdita di sistemi informativi	ALTO	ALTO	MEDIO	BASSO	BASSO	MEDIO	ACCETTARE	BASSO

Azioni non autorizzate
Compromissione dei sistemi informatici di Terze Parti
Denial of service
Errori di configurazione
Exploit del software
Information Gathering
Information leakage
Malware
Social engineering

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:

Report dei rischi per categoria di minaccia

ESEMPIO

Attacchi Logici e/o Fisici

Attacchi al sistema di autenticazione

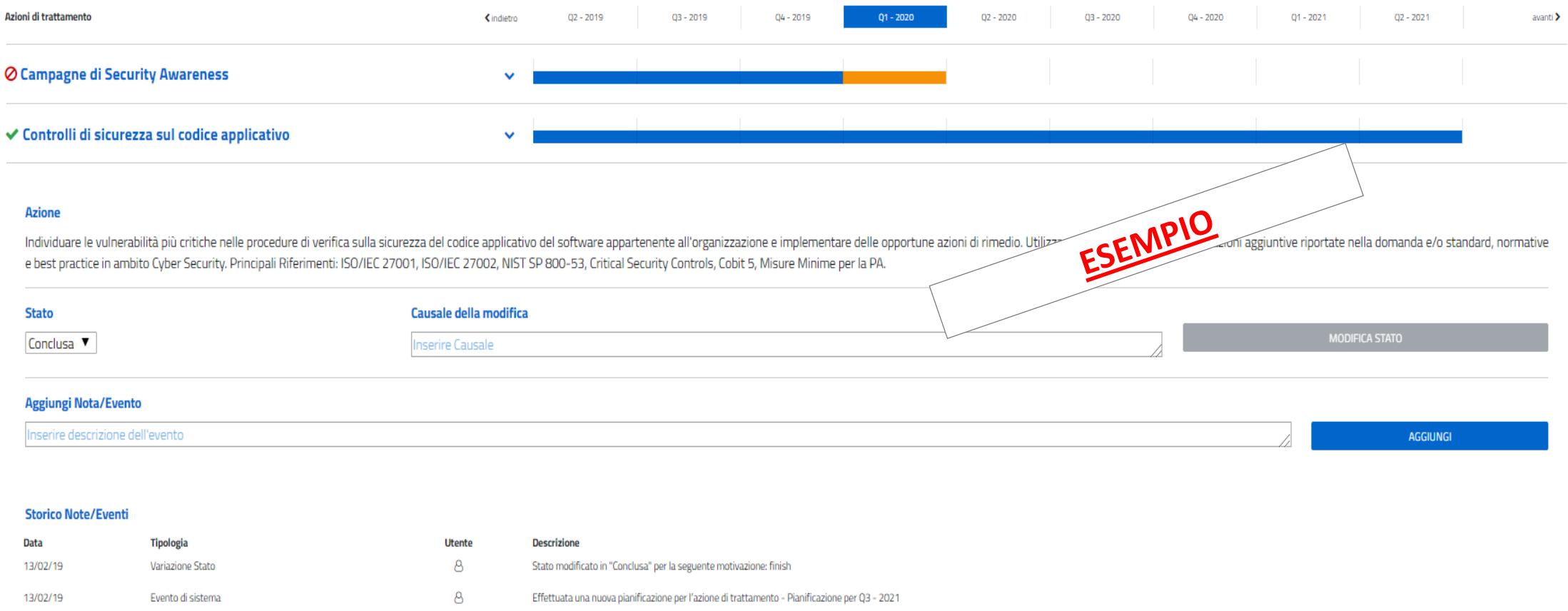
Minaccia	Impatto R-I-D	Vulnerabilità	Esposizione alla minaccia	Probabilità di accadimento	Rischio attuale	Propensione al rischio	Opzioni di trattamento	Rischio derivato
Accesso non autorizzato a credenziali di autenticazione valide	ALTO	ALTO	ALTO	ALTO	ALTO	MEDIO	MITIGARE	ALTO
Session hijacking	ALTO	ALTO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

Monitoraggio continuo del piano dei trattamenti 2/2



AGID | Agenzia per l'Italia Digitale

FormezPA

GRAZIE PER L'ATTENZIONE

rossi@agid.gov.it