



**consip**

# **Le iniziative Consip a supporto del Piano Triennale per l'informatica nella PA**

**SPC Cloud lotto 2 – Servizi di sicurezza**

Palermo, 12 giugno 2018

## Perché è necessaria la sicurezza ICT

### *Lo scenario delle nuove minacce*

- Da attacchi di singoli hacker a gruppi di professionisti finanziati da governi e/o da malavita organizzata
- Azioni e minacce rivolte a:
  - ✓ accesso non autorizzato a informazioni e dati riservati
  - ✓ blocco nell'erogazione di servizi (Sanità, Utilities, ecc...)
  - ✓ presa del controllo di sistemi che erogano e/o monitorano servizi critici
- La maggior parte degli attacchi informatici sono eseguiti con tecniche basilari a danno di infrastrutture non correttamente mantenute
- Fenomeno in costante aumento.  
Nel solo 2016, ad es., sono state rilevate ben 197 nuove famiglie di ransomware, contro le 44 dell'anno precedente

## Le linee di azione richieste

*(Piano Triennale, misure minime AgID)*

### ▪ Piano Triennale

- ✓ Necessità di dotarsi di un Sistema di gestione della sicurezza delle informazioni (SGSI)
- ✓ Individuazione del profilo di sicurezza adeguato alla propria infrastruttura, definito attraverso specifica analisi del rischio

### ▪ «Misure minime per la sicurezza ICT delle Pubbliche amministrazioni» di AgID

- ✓ Inventario dispositivi e software autorizzati e non (sez. 1 e 2)
- ✓ Protezione configurazioni Hw/Sw
- ✓ Valutazione e correzione continua vulnerabilità
- ✓ Difese da malware
- ✓ Protezione dei dati

# General Data Privacy Regulation (GDPR)

- Adeguamento dal 28 maggio 2018 al nuovo Regolamento Europeo sulla protezione dei dati personali («General Data Privacy Regulation»).
- L'impostazione del GDPR pone l'accento sulla tutela dei diritti dell'interessato, introducendo molte novità e aggiornamenti rispetto al D.lgs. 196/03 per quanto riguarda: le **responsabilità** derivanti dagli obblighi da rispettare, i **processi** da implementare, e dal punto di vista disciplinare, attraverso un inasprimento delle **sanzioni**.
- Principali novità introdotte:
  - ✓ Approccio «risk based» - Valutazione d'impatto effettuato su aree specifiche per identificare e minimizzare i rischi di non conformità
  - ✓ «Privacy by design» - Approccio concettuale innovativo che impone l'obbligo di prevedere già in fase di avvio dei progetti gli strumenti a tutela dei dati personali.
  - ✓ Costituzione del «Data Protection Officer» (DPO)

## SPC Lotto 2

### Servizi di Sicurezza

#### Il bando

Procedura ristretta, suddivisa in 4 lotti, per l'affidamento dei servizi di Cloud Computing, di sicurezza, di realizzazione di portali e servizi online e di cooperazione applicativa per la PA. L'iniziativa prevede inoltre servizi innovativi, inclusi quelli per l'identità digitale, quelli per la realizzazione di Open Data e Big Data e lo sviluppo di applicazioni "mobili" e servizi di sicurezza con l'obiettivo di rendere interoperabili tra loro le Amministrazioni.

#### In sintesi...



**STRUMENTO** Contratto quadro



**DURATA** 60 mesi

#### 1 Lotto



**MASSIMALE**

1 600 mln €



**STATO**

Attivo (termine Lug '21)

RTI aggiudicatario: **Leonardo Spa, IBM Italia Spa, Fastweb Spa, Sistemi Informativi Srl**

#### Servizi disponibili

- ➔ **Servizi di «access management»**, per la gestione delle attività di identificazione, autenticazione ed autorizzazione degli utenti dei servizi *online*
- ➔ **Servizi per l'utilizzo di certificati digitali** (firma, timbro, marca temporale, ecc...), erogati in modalità «as a service», volti a favorire la digitalizzazione dei procedimenti amministrativi e la digitalizzazione dei documenti.
- ➔ **Servizi di sicurezza** erogati sia in modalità «as a service» che in modalità «on premise», atti a garantire la sicurezza applicativa e a supportare le Amministrazioni nella prevenzione e gestione degli incidenti informatici e nell'analisi delle vulnerabilità dei sistemi informativi; i servizi di sicurezza includono anche servizi professionali a supporto delle attività delle Unità Locali di Sicurezza o strutture equivalenti delle Pubbliche Amministrazioni.
- ➔ **Servizi Professionali.** Supporto per la realizzazione di attività nell'ambito della sicurezza applicativa, comprese le attività relative ai servizi di monitoraggio



consip

Il Contratto Quadro

# Catalogo servizi di sicurezza applicativa e sicurezza dati

## IDENTITY & ACCESS MGMT

Gestione delle attività di identificazione, autenticazione ed autorizzazione di utenti esterni per l'accesso ai portali dell'Amministrazione

Identity & Access Management

## ANALISI DELLE VULNERABILITA'

Servizi per la prevenzione degli incidenti informatici attraverso l'analisi delle vulnerabilità delle applicazioni per dispositivi sia fissi, sia mobili, durante l'intero ciclo di sviluppo software

Static application security testing

Dynamic application security testing

Mobile application security testing

Vulnerability assessment

## SECURITY OPERATION CENTER (SOC)

Raccolta e correlazione degli eventi; monitoraggio delle infrastrutture di sicurezza e degli incidenti e delle attività sospette.

SOC / Security Information Event Management

## CERTIFICATI DIGITALI

Servizi per l'utilizzo di certificati digitali per favorire la dematerializzazione dei documenti e la gestione digitale dei processi amministrativi

Firma Digitale Remota

Timbro Elettronico

Marche temporali

Certificati SSL

## SERVIZI DI PROTEZIONE

Servizi progettati per la protezione delle Amministrazioni da accessi non autorizzati o violazioni delle policy di sicurezza, riducendo il rischio di sottrazione delle informazioni

Data loss/leak prevention

Web application/Next Generation firewall

Database Security

Secure Web Gateway

## SERVIZI PROFESSIONALI

Supporto nella realizzazione di attività nell'ambito della sicurezza applicativa e cibernetica, comprensive di quelle relative ai servizi di monitoraggio, attraverso l'utilizzo di specifiche figure professionali

## Fruizione dei servizi

### *Modalità operative*

- Nella fase di attivazione dei servizi, l'Amministrazione definisce con il Fornitore la strategia e le *policy* di sicurezza per il blocco delle minacce e i livelli di criticità dei servizi erogati (critici e non critici). Le *policy* possono essere riviste su base esigenza.
- La gestione degli *incident* avviene in funzione delle policy definite e dei relativi livelli di criticità.
- Per i servizi di *assessment* il Fornitore identifica e comunica all'Amministrazione il perimetro che sarà interessato dall'attività di analisi e di test, la tipologia e la descrizione dei controlli effettuati e la valutazione dell'impatto potenziale.
- Il Fornitore emette periodicamente differenti tipologie di *report* sugli eventi monitorati: *executive summary, technical report, remediation plan*.

## Mapping esigenze / servizi a catalogo

(Piano Triennale, misure minime AgID)

- Esecuzioni periodiche di verifica presenze vulnerabilità prodotti e sistemi ICT
- Esecuzioni periodiche integrità software utilizzati
- Difese da *malware* e protezione dati
- Attività di *assessment* e di supporto finalizzate ad individuare esposizioni e azioni di contrasto (supporto CERT-PA, alle ULS, ai SOC)
- Vulnerability Assessment  
Verifica dello stato di sicurezza delle infrastrutture e dello stato delle esposizioni, individuando opportune azioni di rimedio
- Static and Dynamic application security testing  
Identificazione delle vulnerabilità dei *software* sia nel codice sorgente sia in esecuzione
- DLP, DB security, WAF, Secure Web Gateway, SOC  
Protezione dei dati da accessi non autorizzati, *anti-ransomware*, filtro traffico di rete e controllo accessi web
- Servizi Professionali  
Supporto e affiancamento alle Amministrazioni in tutte le attività in ambito



# Mapping esigenze / servizi a catalogo

## GDPR

### Servizi professionali a supporto delle fasi progettuali

- Fase di analisi
  - ✓ Predisposizione del Registro delle operazioni di trattamento contenente tutte le informazioni richieste dalla normativa
- Fase di progettazione
  - ✓ definizione del Sistema di Gestione dei dati personali contenente: modello organizzativo (DPO), processo di «privacy by Design», processo di «data breach notification», processo di «privacy impact assessment», modulistica
  - ✓ predisposizione del piano di implementazione degli interventi.
- Fase di esecuzione
  - ✓ Supporto alla stesura di processi e procedure.
  - ✓ Analisi, valutazione e gestione del rischio.
  - ✓ Progettazione e valutazione di architetture tecnologiche di sicurezza per la mitigazione della componente di rischio ICT.
  - ✓ Supporto alle attività di audit e alla gestione dei «data breach»
  - ✓ Training





**consip**

acquistiamo valore per l'Italia

**Roberto Bettacchi**  
Divisione Sourcing ICT – ICT Strategico

**Consip S.p.A.**  
Via Isonzo 19/E – 00198 Roma  
T +39 0685449.1

roberto.bettacchi@consip.it

**www.consip.it**



@Consip\_Spa



[www.linkedin.com/company/consip/](http://www.linkedin.com/company/consip/)



Canale "Consip"