AIIC2023
FORTEZZA DA BASSO
Firenze 10-13 maggio 2023
Convegno Nazionale
Associazione Italiana Ingegneri Clinici
Innovazione e accessibilità:
il governo delle tecnologie sanitarie come sfida sociale
1993 - 2023

Ricadute sul procurement degli aspetti di cybersecurity e regolatori

Ing. Davide Salute

davide.salute@asugi.sanita.fvg.it

Azienda Sanitaria Universitaria Giuliano Isontina (ASUGI) - Trieste

Cybersecurity: il contesto

Il quadro legislativo generale:

- 25/5/2018: diretta applicabilità del GDPR → cambiate le regole e le responsabilità per il trattamento dei dati personali

- 26/05/2021: nuovo regolamento sui dispositivi medici MDR → cambiate le regole e le responsabilità nell'approccio ai DM
- 26/05/2022: nuovo regolamento sui dispositivi medici diagnostici in vitro IVDR → cambiate le regole e le responsabilità nell'approccio agli IVD

- 01/04/2023: entrata in vigore il Nuovo Codice degli Appalti. Dal 1 luglio 2023 verrà abrogato il D.Lgs. 50/2016.

Cybersecurity: il contesto

Il quadro regolatorio per la Sicurezza Cibernetica:

- Direttiva 2016/1148 (c.d. Direttiva NIS "Network and Information Security")
  - al fine di conseguire un "livello elevato di sicurezza della rete e dei sistemi informativi in ambito nazionale, contribuendo ad incrementare il livello comune di sicurezza nell'Unione Europea"
  - recepita con D.Lgs. 65/2018, che detta la cornice legislativa delle misure da adottare ed individua i soggetti competenti per dare attuazione agli obblighi NIS:
    - Autorità Nazionale NIS -> Settore Salute = Ministero della Salute
    - Autorità Regionale NIS -> Settore Salute = Ente Regione
    - Operatori di Servizi Essenziali OSE -> ENTI SANITARI
- Conferenza Stato Regioni 07/11/2019 adotta: "Autorità NIS - Settore Salute Linee Guida per gli Operatori di Servizi Essenziali (OSE)" v1.0 16/07/2019
  - Framework Nazionale di Cyber Security e la Data Protection (v2.0 Febbraio 2019), predisposto dal CINI Cybersecurity National Lab (Consorzio Interuniversitario Nazionale per l'informatica) e dal CIS-Sapienza (con supporto di Garante Privacy e DIS-PCM)
  - Gestione del ciclo di vita del processo della Cybersecurity
  - 5 Funzioni: Identify/Protect/Detect/Respond/Recover; 117 Controlli
  - Sintesi calata nel contesto italiano dei principali framework: NIST e ISO/IEC 27001, ma anche COBIT, ISA, GDPR, CIS e Misure Minime AgID

Cybersecurity: il contesto

Il quadro regolatorio per la Sicurezza Cibernetica:

- ACN – Agenzia per la Cybersicurezza Nazionale (D.L. n. 82/2021)
  - L'adozione del D.L. 14 giugno 2021, n. 82 ha ridefinito l'architettura nazionale cyber e istituito l'Agenzia per la Cybersicurezza Nazionale (ACN), a tutela degli interessi nazionali nel campo della cybersicurezza ed in attuazione di precisi obiettivi del PNRR

  - L'ACN assicura il coordinamento tra i soggetti pubblici coinvolti nella gestione delle cybersicurezza

  - 01/09/2021 - Avvio prima operatività
  - 16/09/2021 - Incorpora CSIRT Italia (Computer Security Incident Response Team) e CVCN (Centro di Valutazione e Certificazione Nazionale), compresi i ruoli di ricezione notifiche PSNC
  - 30/06/2022 - Trasferimento di funzioni in materia di cybersicurezza di MISE
  - Ottobre 2022 - Trasferimento di funzioni in materia di cybersicurezza di AgID

Cybersecurity: il contesto

Il quadro regolatorio per la Sicurezza Cibernetica:

- Il paradigma «Cloud First» per la PA

"Piano Triennale per l'informatica nella Pubblica Amministrazione" AgID - I Ed. 2017-2019: a seguito del primo censimento dei datacenter della PA 2013, nasce il concetto di «Cloud della PA» da cui:

- esperimento SPC-Cloud Lotto 1 (OpenStack) (servizi IaaS/Paas);
- il/i Polo/i Strategico/ci Nazionale/i (PSN) (servizi IaaS/PaaS);
- i Cloud Service Provider (CSP) (servizi SaaS/IaaS/PaaS) qualificati sul «Cloud Marketplace di AgID» che non è un marketplace -> dal 19 gennaio 2023 «Cloud Marketplace di ACN»

- Esclusioni (per ora): CIRCOLARE N. 01 del 14 giugno 2019

Le istituzioni universitarie, gli enti di ricerca e gli enti appartenenti al Sistema Sanitario Nazionale possono procedere all'acquisizione di beni e servizi ICT per i propri Data Center, previa comunicazione ad AGID, ai soli fini di:

- ricerca, sviluppo e trasferimento tecnologico;
- supporto della diagnostica clinica.

Cybersecurity: il contesto

Il quadro regolatorio per la Sicurezza Cibernetica:

- Il paradigma «Cloud First» per la PA

  La «**Strategia Cloud Italia per la PA**» di ACN

  - 01/09/2021 costituzione di ACN -> 07/09/2021 Stategia Cloud

- Pillar 1:

la Classificazione di dati e servizi (Ordinari/Critici/Strategici) -> in Sanità «Ordinari» e «Critici»

- Pillar 2:

La Qualificazione ex-ante dei servizi Cloud acquisibili dalla PA

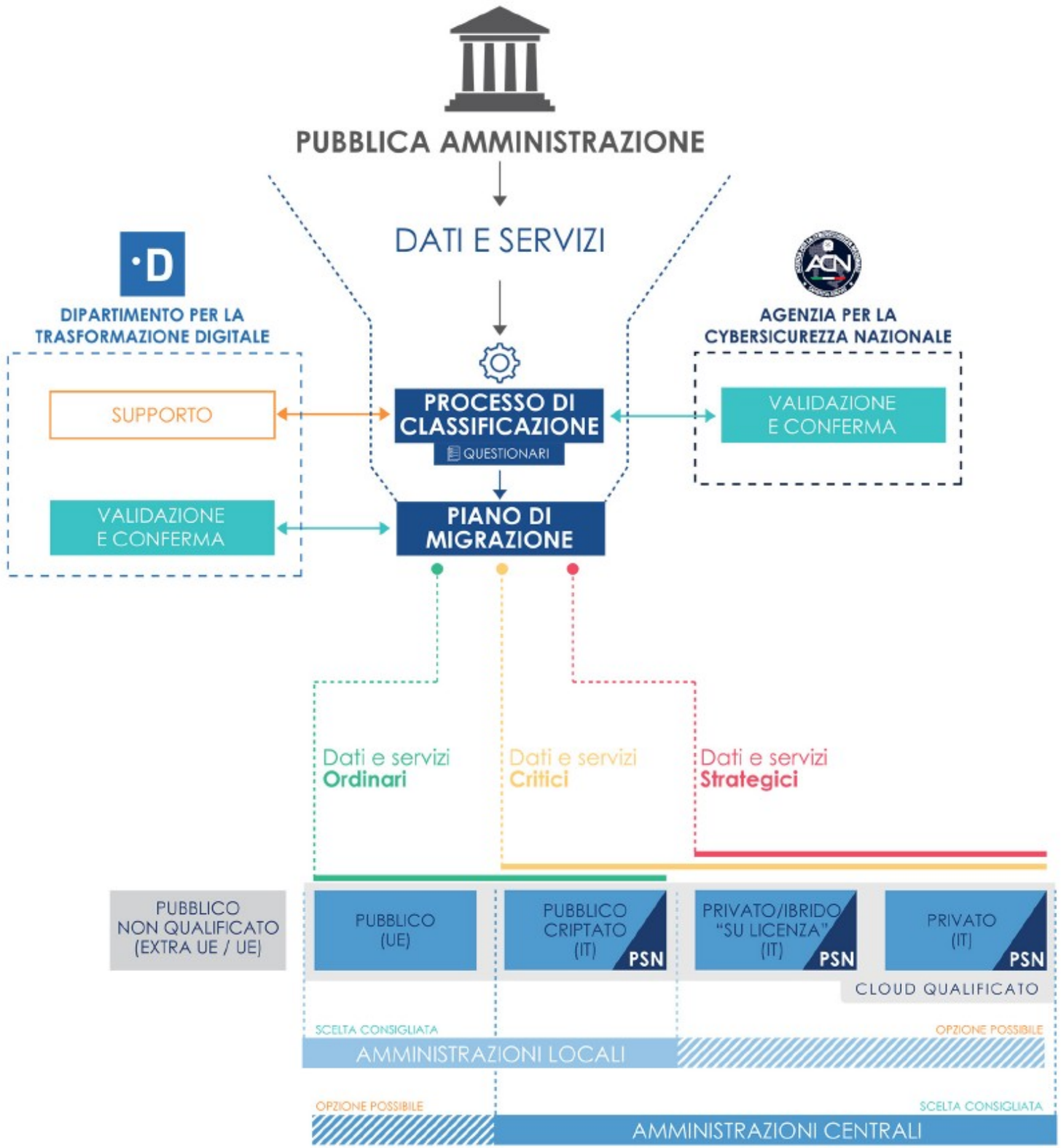
- Pillar 3:

Il Polo Strategico Nazionale (PSN)

  - Fase 1 e 2: realizzazione PSN entro 2022
  - Fase 3: migrazione PA entro il 2025

Cybersecurity: il contesto

La «Strategia Cloud Italia per la PA» di ACN



<u>Acquisto di servizi cloud</u>:

- Servizi SaaS Ordinari e Critici
  -> Marketplace ACN

- Servizi IaaS Ordinari
  -> Marketplace ACN - Cloud Pubblico UE

- Servizi IaaS Critici
  -> Marketplace ACN - Cloud Pubblico Criptato
  -> PSN

Cybersecurity: il contesto

Il quadro regolatorio per la Sicurezza Cibernetica:

- Il PSN (GDPR e NIS compliance)
  - PNRR: Investimenti 1.1 e 1.2:

- Il panorama completo dei Servizi PSN:
  - Connettività
  - Housing (anche trasporto assicurato)
  - Hosting
  - Cloud Privato (Iaas/PaaS/CaaS)
    - HA e DR
    - Storage e backup
  - Hybrid Cloud on PSN site (hyperscaler licenziato da uno o più CSP)
  - Secure Public Cloud on Microsoft Azure Google GCP
  - Public Cloud PSN Managed
  - Servizi Professionali e Operation

Cybersecurity: come orientarsi

Cosa abbiamo capito:

- Che il quadro regolatorio è molto articolato e mutevole: legislatore (nazionale e UE) in fibrillazione sul tema cybersecurity

- Che gli adempimenti sono molti, con perimetro e contenuti difficili da individuare e monitorare nel tempo (scadenze, adempimenti, ecc)
  - Necessità di uffici preposti/dedicati (Operation vs Security&Compliance)
- I Dispositivi Medici e gli Apparecchi Elettromedicali rientrano nel perimetro

- E' necessario adottare misure tecniche ed organizzative importanti e tutto questo ha un *effort* su di noi e deve trovare una corrispondenza su PROCUREMENT e CONTRATTI

Cybersecurity: come orientarsi- Ripartiamo dal documento
ENISA (European Union Agency for Network and Information Security)
Smart Hospitals- NOV 2016
Security and Resilience for Smart Health Service and Infrastructures

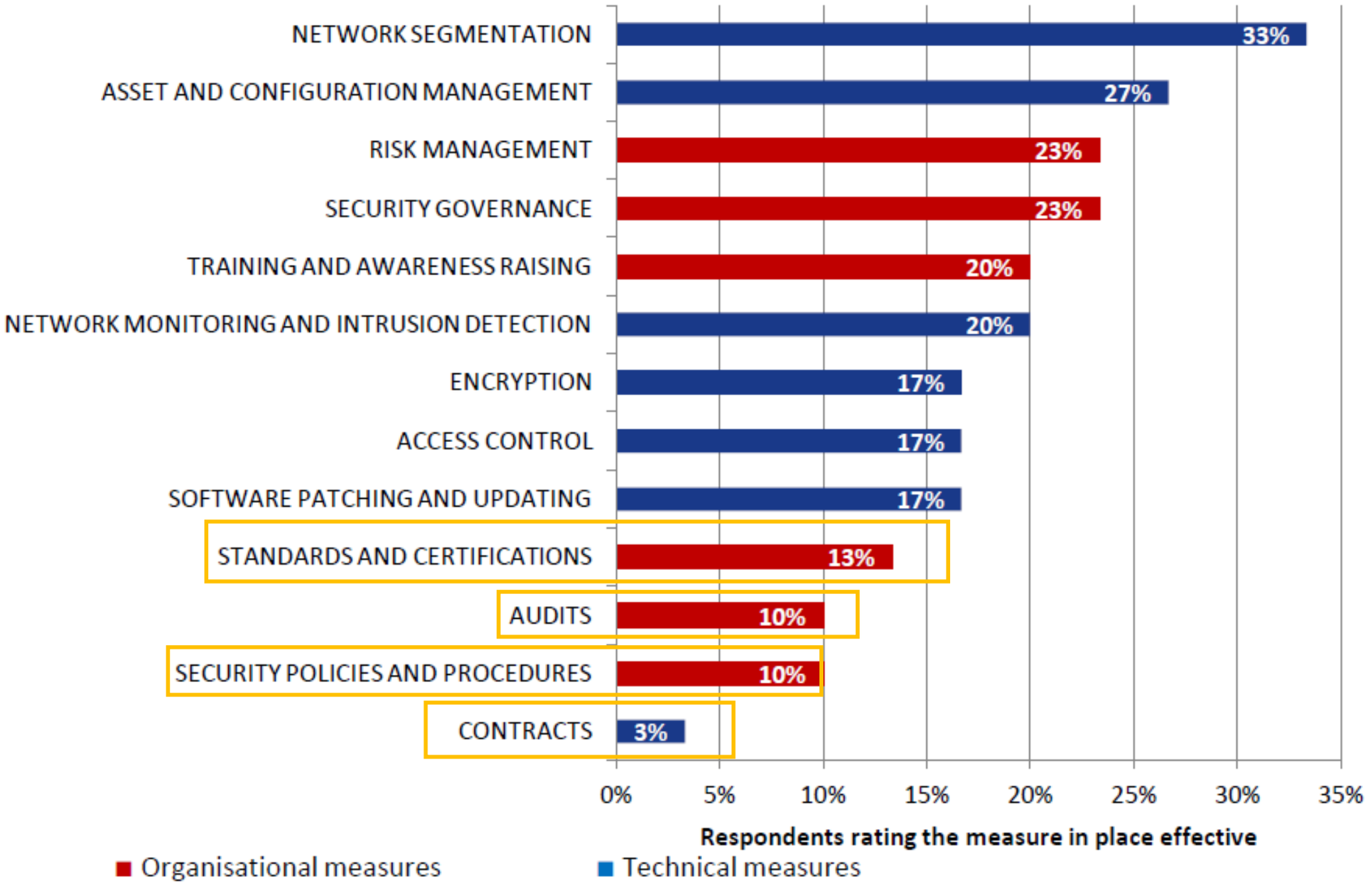


Figure 15 Effective measures in place

Cybersecurity: come rispondere

- Maggiore attenzione agli aspetti contrattuali (**CONTRACTS**)
  - Linee guida AgID «La sicurezza nel procurement ICT» Aprile 2020
  - Implicazioni del quadro regolatorio:
    - GDPR -> DPIA, Nomina Responsabile (contenuti)
    - NIS -> Ciascuno dei 117 controlli ha delle implicazioni nel contratto, sia tecniche che organizzative (supporto dal fornitore)
    - Cloud ->
      - C'è?
      - E' SaaS qualificato?
      - PSN: housing, hosting, IaaS?
      - Se SaaS o infrastruttura On-Premise (in housing su PSN) i

Linee guida AgID «La sicurezza nel procurement ICT» Aprile 2020

Al contrario, per acquisizioni classificate di alta criticità, l'amministrazione potrebbe ad esempio verificare che eventuali accordi quadro disponibili (come oggetto e capienza) prevedano requisiti di sicurezza adeguati per quel grado di criticità: in caso la verifica sia negativa, l'amministrazione potrebbe scartare l'opzione di servirsi del suddetto accordo quadro. NB: occorre ricordare che, per la loro stessa natura, gli accordi quadro sono strumenti di tipo "generalista", pertanto potrebbero contenere requisiti di sicurezza adeguati alla maggioranza dei casi ma non per specifiche iniziative dell'amministrazione.

Linee guida AgID «La sicurezza nel procurement ICT» Aprile 2020

PS1 Richiama Linee Guida AgID «Sviluppo Sicuro del Software»

PS2 Sono tutti aspetti che vanno definiti e regolamentati in maniera chiara in capitolato, ma soprattutto in fase di analisi pre-gara…

Come rispondere

-Maggiore attenzione agli aspetti contrattuali (**CONTRACTS**)

Domanda: cosa stiamo comprando?

E' presente una infrastruttura IT? Un Server? Un Appliance?

Prendere in considerazione in fase di gara RTO ed RPO dei sistemi IT medicali offerti (sia cloud che on-premice):

valori minimi e valori proposti dal mercato

Concetti legati a Continuità Operativa e Disaster Recovery delle infrastrutture IT. Rappresentano in maniera intuitiva i livelli di servizio attesi sulla base delle specifiche di progetto

-RTO (Recovery Time Objective): quanto tempo sono disposto ad aspettare per tornare operativo?

-RPO (Recovery Time Objective): quanti dati sono disposto a constatare di aver perso dopo che sono tornato operativo?

-> RTO e RPO = 0

Come rispondere

-Maggiore attenzione agli aspetti contrattuali (**CONTRACTS**)

Domanda: cosa stiamo comprando?

E' presente un software?

Prendere in considerazione in fase di gara la Software Security Validation (SSV) anche detto Testing del Codice (Statico e Dinamico): da eseguire almeno sui software collegati a vario titolo ad un DM o DM SW e installati sui PC/server aziendali

Perché?

-In applicazione del modello Zero Trust: devo verificare il sw o limitarne gli effetti come fosse non sicuro, unica alternativa alla SSV è la virtualizzazione applicativa (costi, complessità)

-In applicazione delle Misure Minime di sicurezza ICT per le PA: whitelist applicazioni consentite (E VALIDATE)

-«Il *Software* è come una scatola di cioccolatini… non sai mai quello che ti capita!»

Futuro: SaaS?

AIIC2023
FORTEZZA DA BASSO
Firenze 10-13 maggio 2023
Convegno Nazionale
Associazione Italiana Ingegneri Clinici
Innovazione e accessibilità:
il governo delle tecnologie sanitarie come sfida sociale
30 AIIC 1993 - 2023

Ricadute sul procurement degli aspetti di cybersecurity e regolatori

Ing. Davide Salute
davide.salute@asugi.sanita.fvg.it
Azienda Sanitaria Universitaria Giuliano Isontina (ASUGI) - Trieste

GRAZIE DELL'ATTENZIONE!