AgID per la Cybersecurity della Pubblica Amministrazione

Le Misure Minime di sicurezza ICT per le Pubbliche amministrazioni

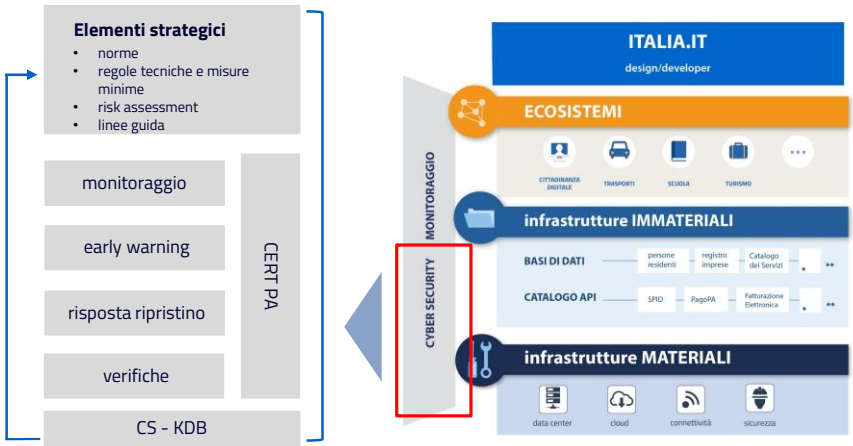
Corrado Giustozzi
Agenzia per l'Italia Digitale – CERT-PA

Security Summit Roma, 8 giugno 2017

Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri

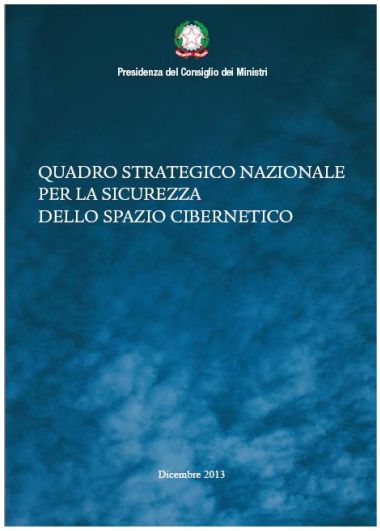
La CyberSecurity nel modello ICT per la PA

Il ruolo dei CERT e di AgID nella gestione della sicurezza



Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri

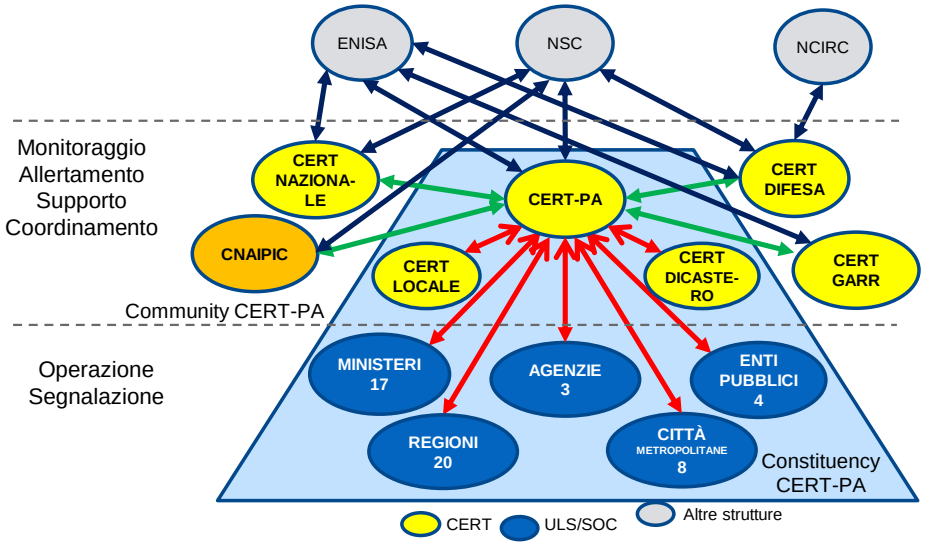
Il ruolo di AgID nel QSN



- Regole tecniche e linee guida
- Protezione del patrimonio informativo
- Razionalizzazione dei CED
- Servizi erogati dalle Pubbliche Amministrazioni
- Formazione
- CERT-PA

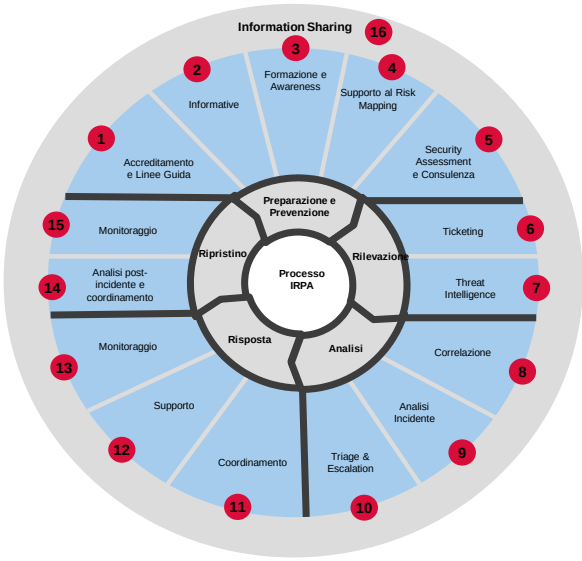
Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri

Il ruolo del CERT-PA



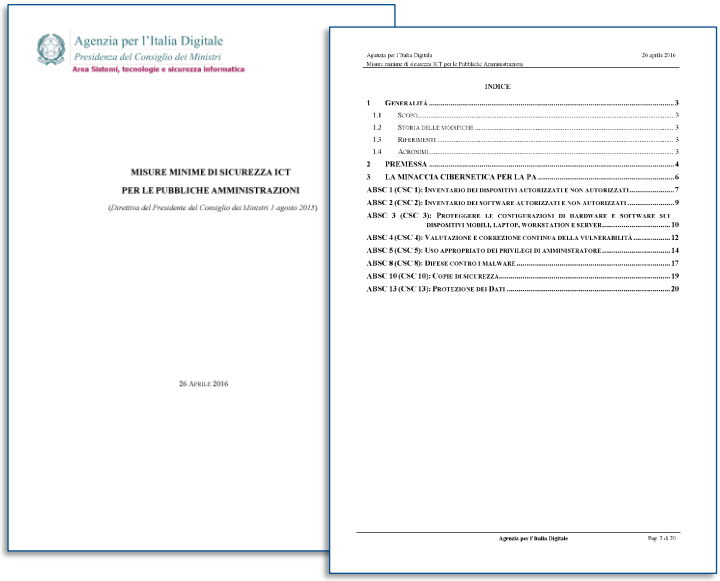
Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri

I servizi del CERT-PA



- PAC
- Regioni
- Città metropolitane
- Tutto il resto (.gov.it)

Le Misure Minime di sicurezza



Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri
Area Sistemi, tecnologie e sicurezza informatica

MISURE MINIME DI SICUREZZA ICT
PER LE PUBBLICHE AMMINISTRAZIONI
(Direttiva del Presidente del Consiglio dei Ministri 1 agosto 2015)

26 APRILE 2016

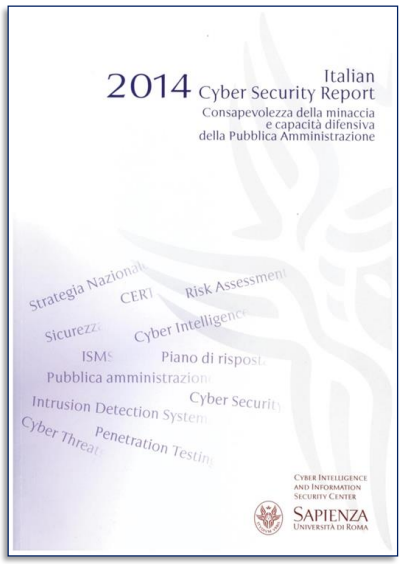
Agenzia per l'Italia Digitale — 26 aprile 2016
Misure minime di sicurezza ICT per le Pubbliche Amministrazioni

INDICE

Agenzia per l'Italia Digitale — Pag. 2 di 20

- Già anticipate via Web sin da settembre 2016
- Emesse con circolare 18 aprile 2017, n. 2/2017
- Gazzetta Ufficiale (SG) n.103 del 5/5/2017
- Adozione obbligatoria entro il 31/12/2017
- Dovere d'ufficio del Dirigente responsabile IT (art. 17 CAD)

I razionali: la situazione nella PA



- Sicurezza basata sulle tecnologie
- Mancanza di strutture organizzative in grado di gestire gli eventi e rispondere agli attacchi
- Superficie d'attacco eccessiva
- Mancanza di una *baseline* comune di riferimento

I livelli di applicazione

Minimo

È quello al quale **ogni pubblica amministrazione**, indipendentemente dalla sua natura e dimensione, **deve necessariamente essere o rendersi conforme.**

Standard

Può essere assunto come **base di riferimento nella maggior parte dei casi.**

Avanzato

Deve essere adottato dalle **organizzazioni maggiormente esposte a rischi** (ad esempio per la criticità delle informazioni trattate o dei servizi erogati), ma anche visto come **obiettivo di miglioramento** da parte di tutte le altre organizzazioni.

Le modalità di applicazione

- Il raggiungimento di elevati livelli di sicurezza, quando è molto elevata la complessità della struttura e l'eterogeneità dei servizi erogati, può essere eccessivamente oneroso se applicato in modo generalizzato. Pertanto **ogni Amministrazione dovrà avere cura di individuare al suo interno gli eventuali sottoinsiemi, tecnici e/o organizzativi, caratterizzati da omogeneità di requisiti ed obiettivi di sicurezza, all'interno dei quali potrà applicare in modo omogeneo le misure adatte** al raggiungimento degli obiettivi stessi.

Le famiglie di controlli

- **ABSC 1** (CSC 1): inventario dei dispositivi autorizzati e non autorizzati
- **ABSC 2** (CSC 2): inventario dei software autorizzati e non autorizzati
- **ABSC 3** (CSC 3): proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server
- **ABSC 4** (CSC 4): valutazione e correzione continua della vulnerabilità
- **ABSC 5** (CSC 5): uso appropriato dei privilegi di amministratore
- **ABSC 8** (CSC 8): difese contro i malware
- **ABSC 10** (CSC 10): copie di sicurezza
- **ABSC 13** (CSC 13): protezione dei dati

ABSC 1 (CSC 1): inventario dei dispositivi autorizzati e non autorizzati

Gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso

- **Inventario delle risorse**
- **Logging**
- **Autenticazione di rete**

ABSC 2 (CSC 2): inventario dei software autorizzati e non autorizzati

Gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione

- **Inventario dei software autorizzati**
- **Whitelist delle applicazioni autorizzate**
- **Individuazione di software non autorizzato**
- **Isolamento delle reti (air-gap)**

ABSC 3 (CSC 3): proteggere le configurazioni di hardware e software sui dispositivi

Istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilità di servizi e configurazioni.

- **Configurazioni standard**
- **Accesso amministrativo da connessioni protette**
- **Verifica dell'integrità dei file critici**
- **Gestione delle configurazioni**

ABSC 4 (CSC 4): valutazione e correzione continua della vulnerabilità

Acquisire, valutare e intraprendere continuamente azioni in relazione a nuove informazioni allo scopo di individuare vulnerabilità, correggere e minimizzare la finestra di opportunità per gli attacchi informatici.

- **Verifica delle vulnerabilità**
- **Aggiornamento dei sistemi**

ABSC 5 (CSC 5): uso appropriato dei privilegi di amministratore

Regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi.

- **Limitazione dei privilegi delle utenze amministrative**
- **Inventario delle utenze amministrative**
- **Gestione delle credenziali delle utenze amministrative**

ABSC 8 (CSC 8): difese contro i malware

Controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive.

- **Sistemi di protezione (antivirus, firewall, IPS)**
- **Uso dei dispositivi esterni**
- **Controllo dei contenuti Web, email**

ABSC 10 (CSC 10): copie di sicurezza

Procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità.

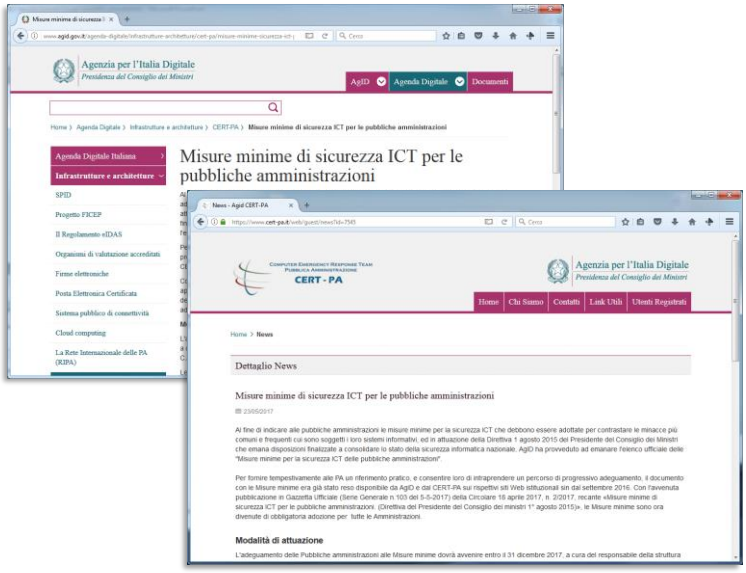
- **Backup e verifica del restore**
- **Protezione delle copie di backup**

ABSC 13 (CSC 13): protezione dei dati

Processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti

- **Uso della crittografia**
- **Limitazioni sull'uso di dispositivi removibili**
- **Controlli sulle connessioni di rete/Internet**

Risorse on line



- Sui siti Web di AgID e del CERT-PA sono disponibili:
  - la normativa
  - i moduli in formato elettronico editabile
- Riferimenti:
  - www.agid.gov.it
  - www.cert-pa.it

Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri

Il Paese che cambia passa da qui.

agid.gov.it