



Le Misure Minime di sicurezza ICT per le Pubbliche Amministrazioni

Corrado Giustozzi

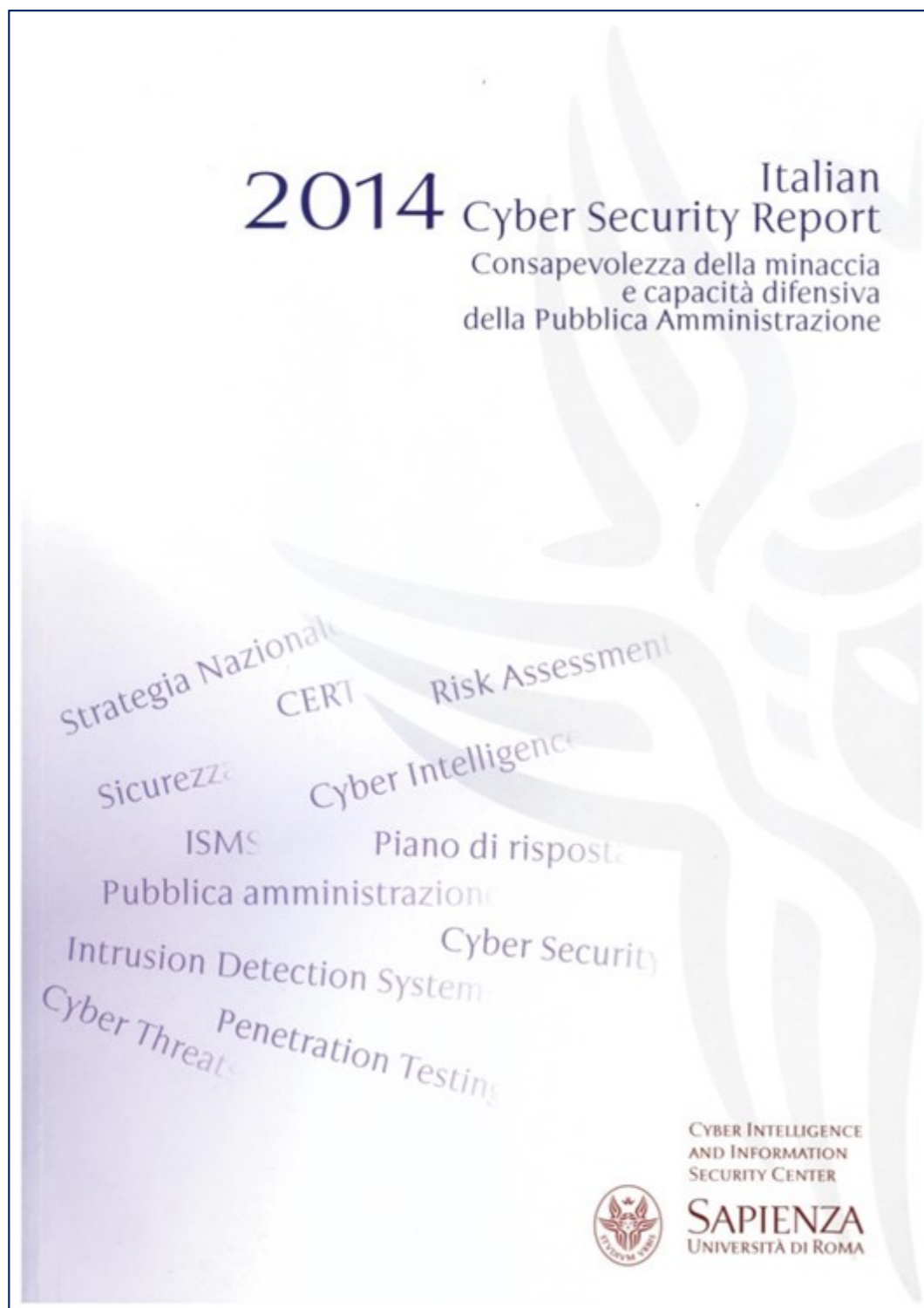
*Esperto di sicurezza cibernetica presso l'Agenzia per l'Italia Digitale
per lo sviluppo del CERT della Pubblica Amministrazione (CERT-PA)*



Formez, 6 febbraio 2018

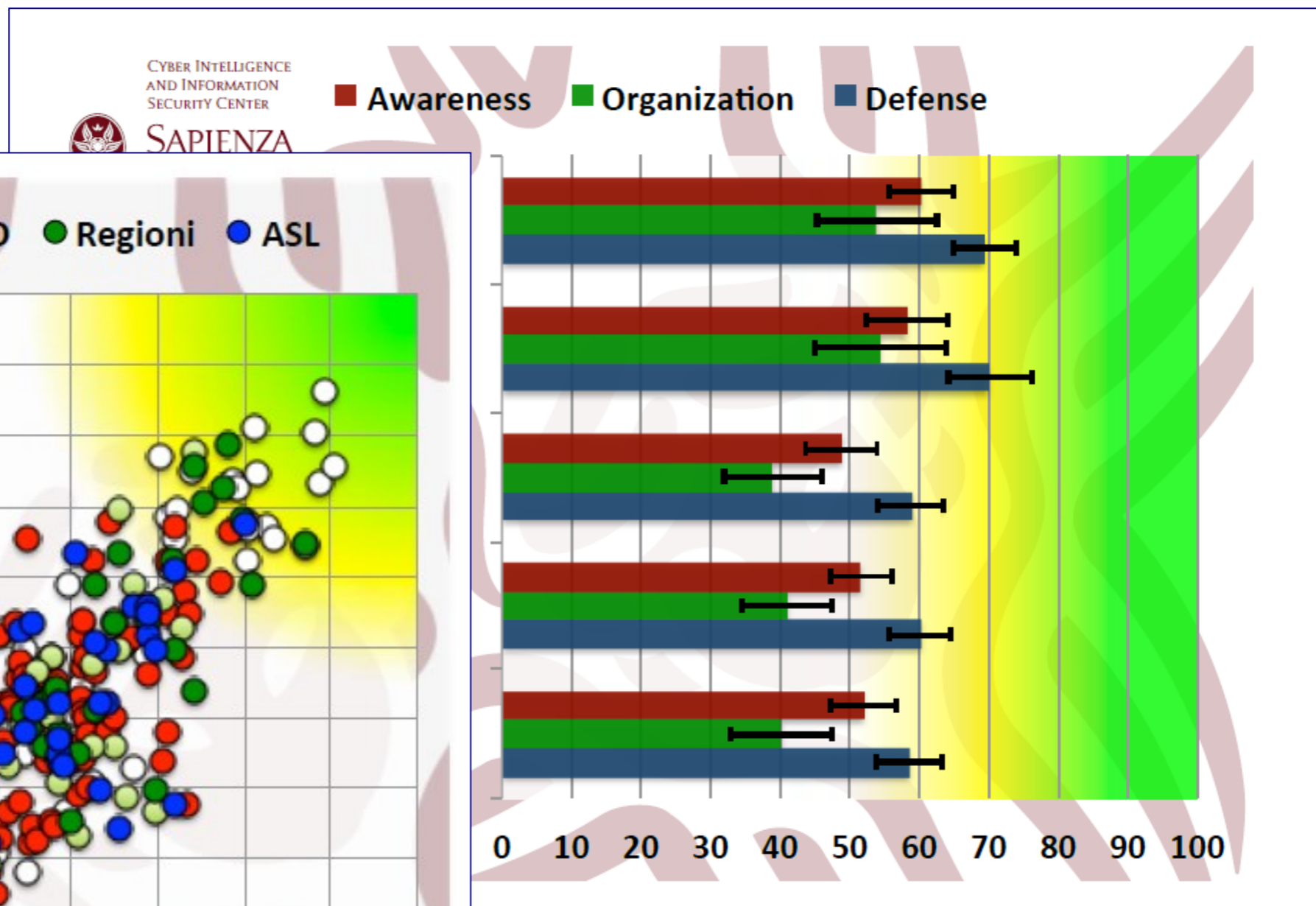


I razionali: la situazione nella PA



- 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

Una Pubblica Amministrazione vulnerabile





Le Misure Minime di sicurezza

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

MISURE MINIME
PER LE PUBBLICHE AMMINISTRAZIONI
(Direttiva del Presidente della Repubblica)

26 aprile 2016

Agenzia per l'Italia Digitale
 Misure minime di sicurezza ICT per le Pubbliche Amministrazioni

INDICE

1 GENERALITÀ	3
1.1 SCOPO.....	3
1.2 STORIA DELLE MODIFICHE.....	3
1.3 RIFERIMENTI.....	3
1.4 ACRONIMI.....	3
2 PREMESSA	4
3 LA MINACCIA CIBERNETICA PER LA PA	6
ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI	7
ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI	9
ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER	10
ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ	12
ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE	14
ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE	17
ABSC 10 (CSC 10): COPIE DI SICUREZZA	19
ABSC 13 (CSC 13): PROTEZIONE DEI DATI	20

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**
- **Publicate in 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)**



Obiettivi

Indirizzare l'esigenza delle Amministrazioni fornendo loro, in particolare a quelle meno preparate, un riferimento operativo direttamente utilizzabile (checklist) nell'attesa della pubblicazione di documenti di indirizzo di più ampio respiro

Stabilire una baseline comune di misure tecniche ed organizzative irrinunciabili

Fornire alle Amministrazioni uno strumento per poter verificare lo stato corrente di attuazione delle misure di protezione contro le minacce informatiche, e poter tracciare un percorso di miglioramento

Responsabilizzare le Amministrazioni sulla necessità di migliorare e mantenere adeguato il proprio livello di protezione cibernetica ponendo il compito (e la relativa responsabilità) direttamente in capo al dirigente competente



Considerazioni ispiratrici

Non reinventare la ruota ma basarsi su esperienze consolidate (SANS 20 / CSC)

Indirizzare le caratteristiche e le esigenze specifiche delle nostre Pubbliche Amministrazioni

Minimizzare gli impatti implementativi (*effort*, costi)

Fornire requisiti in linea con le più diffuse e consolidate *best practice* di settore

Armonizzare il quadro a valle del GDPR e della direttiva NIS



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



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



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

Controlli principali:

- 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

Controlli principali:

- 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.

Controlli principali:

- 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.

Controlli principali:

- **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.

Controlli principali:

- 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.

Controlli principali:

- 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.

Controlli principali:

- 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

Controlli principali:

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



Risorse on line

The screenshot shows the AgID website page titled 'Misure minime di sicurezza ICT per le pubbliche amministrazioni'. The page content includes:

- Agenda Digitale Italiana**
- Infrastrutture e architetture**
- SPID**
- Progetto FICEP**
- Il Regolamento eIDAS**
- Organismi di valutazione accreditati**
- Firme elettroniche**

The main text on the page discusses the measures for ICT security for public administrations, mentioning the 1 August 2015 Directive and the 18 April 2017 Circular.

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

The screenshot shows the CERT-PA website page titled 'Misure minime di sicurezza ICT per le pubbliche amministrazioni'. The page content includes:

- COMPUTER EMERGENCY RESPONSE TEAM PUBBLICA AMMINISTRAZIONE CERT - PA**
- Home**
- Chi Siamo**
- Contatti**
- Link Utili**
- Utenti Registrati**

The main text on the page is identical to the AgID page, discussing the measures for ICT security for public administrations.



www.agid.gov.it
corrado.giustozzi@agid.gov.it

www.cert-pa.it
cert-pa@cert-pa.it



COMPUTER EMERGENCY RESPONSE TEAM
PUBBLICA AMMINISTRAZIONE

CERT - PA